

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Child Safe Viewing Act;)	
Examination of Parental Control Technologies for)	MB Docket No. 09-26
Video or Audio Programming)	
)	

**COMMENTS OF ADAM THIERER,
SENIOR FELLOW WITH THE PROGRESS & FREEDOM FOUNDATION ("PFF")
AND THE DIRECTOR OF PFF'S CENTER FOR DIGITAL MEDIA FREEDOM**

Adam D. Thierer
The Progress & Freedom Foundation
1444 Eye St., NW Suite 500
Washington, DC 20005
202-289-8928
athierer@pff.org
www.pff.org

April 16, 2009

TABLE OF CONTENTS

I.	INTRODUCTION: UNDERSTANDING THE ROLE AND LIMITS OF PARENTAL CONTROLS.....	2
	A. No System is Foolproof and This is Not an Exact Science.....	2
	B. There Is No Reason to Believe that a Government-Mandated Solution Would Be Preferable to Private Controls.....	4
	C. The Goal Should Be ‘Let-a-Thousand-Flowers-Bloom,’ Not ‘One-Size-Fits All’	6
	D. Thinking in Terms of Training Wheels and Speed Bumps	7
II.	ACCESSING THE RELEVANT UNIVERSE OF PARENTAL CONTROL USERS	8
	A. Calculating How Many Homes Have Children Present	9
	B. Homes with Very Young or Much Older Children Have Less Need for Controls.....	11
	C. For a Variety of Reasons, Some Families Opt to Never Use Parental Controls	14
	D. The Big Picture: Only a Small Percentage of Homes Need Parental Controls	15
III.	A SURVEY OF THE MARKETPLACE FOR PARENTAL CONTROL TOOLS AND RATING SYSTEMS	16
	A. Television	16
	B. Movies.....	38
	C. Music and Radio.....	43
	D. Video Games	48
	E. Wireless & Mobile Media	62
	F. Internet & Social Networking Sites.....	71
IV.	THE PERILS OF MANDATORY CONTROLS, RESTRICTIVE DEFAULTS OR “UNIVERSAL” RATINGS.....	98
	A. Why Mandatory Controls or Defaults Will Backfire	99
	B. Why Mandating Universal Ratings Would Be a Mistake	110

V.	WHY MANDATORY AGE VERIFICATION WON'T WORK AND WOULD MAKE KIDS LESS SAFE	119
A.	Age Verification Regulation Has Already Been the Subject of a Protracted Legal Battle.....	120
B.	Blue Ribbon Online Safety Task Forces Agree that Mandatory Age Verification is Not Workable, Will Not Improve Online Child Safety	122
C.	Ten Problems with Mandatory Age Verification as a Solution to Online Safety Concerns	123
D.	Summary of Potential Problems with Age Verification Mandates.....	128
VI.	THE IMPORTANCE OF HOUSEHOLD MEDIA RULES	129
A.	“Where” Rules	130
B.	“When and How Much” Rules	131
C.	“Under What Condition” Rules.....	132
D.	“What” Rules.....	134
VII.	THE ROLE OF THIRD-PARTY PRESSURE, RATINGS AND ADVICE	135
A.	The Power of Public Pressure & Social Norms.....	135
B.	Independent Media Rating Efforts	138
VIII.	THE POWER OF THE PURSE AND MEDIA ALLOWANCES	142
IX.	JURISDICTIONAL AND FIRST AMENDMENT CONSIDERATIONS.....	143
A.	Jurisdictional Considerations	143
B.	First Amendment Constraints.....	143
X.	CONCLUSION.....	147

EXECUTIVE SUMMARY

Pursuant to the requirements set forth by the Child Safe Viewing Act of 2007,ⁱ the Federal Communications Commission (“the Commission”) has undertaken a review of the marketplace for “advanced blocking technologies.”ⁱⁱ This inquiry provides the Commission with the opportunity to highlight the amazing advances, and continuing challenges, in the marketplace for parental control technologies.

I have spent over 15 years monitoring developments in this field and my research has culminated in the publication by The Progress & Freedom Foundation (“PFF”) of an ongoing, and constantly growing, special report, *Parental Controls & Online Child Protection: A Survey of Tools and Methods*.ⁱⁱⁱ I offer the following conclusions drawn from my research that may be relevant to the Commission’s *NOI*:

- **There exists an unprecedented abundance of parental control tools:** There has never been a time in our nation’s history when parents have had more tools and methods at their disposal to help them decide what constitutes acceptable media content in their homes and in the lives of their children. Parents have been empowered with technologies, strategies, and information that can help them devise and enforce a media plan for their families that is in line with their own needs and values. Simply stated, this is a well-functioning marketplace. [see Section III]

ⁱ Child Safe Viewing Act of 2007, S. 602, P.L. 110-452, 122 Stat. 5025, December 2, 2008 (hereinafter Child Safe Viewing Act).

ⁱⁱ Federal Communications Commission, Notice of Inquiry In the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming, FCC 09-14, MB Docket No. 09-26, March 2, 2009 (hereinafter FCC, Child Safe Viewing Act Notice).

ⁱⁱⁱ Adam Thierer, *Parental Controls and Online Child Protection: A Survey of Tools and Methods* (Washington, DC: The Progress & Freedom Foundation, Version 3.1, 2008).

- **No parental control tool is foolproof:** Although the quantity and quality of parental control tools constantly expands and improves, with enough effort, most controls can be cracked or circumvented. This will *always* be the case, however, even if the government was designing the tools or requiring their use. Technologies, markets, and artistic expression all evolve, and they do so at an increasingly rapid pace in our modern Information Age. This creates an endless “cat-and-mouse” game. Perfect “control” or “blocking,” therefore, is an unrealistic goal. [see Section I]
- **Rating systems are not an exact science:** Media rating and content-labeling efforts are not an exact science; they are fundamentally subjective exercises. Ratings are based on value judgments made by humans who all have somewhat different values. Those doing the rating are being asked to evaluate artistic expression and assign labels to it that provide the rest of us with some rough proxies about the nature of that particular piece of art, or what age group should (or should not) be consuming it. Consequently, all rating systems will be inherently “flawed” since humans have different perspectives and values that they will use to label or classify content. [see Section I]
- **A rating system is meant to inform, not censor.** Many critics mistake the purpose of a rating system. A rating system (a) is meant to convey information about a given media product to consumers (especially parents), (b) so that they are able to make an informed judgment about the wisdom of consuming that media, or allowing children to consume it. In other words, a good rating system *informs and empowers*. A rating system is *not* a tool to “clean up” or self-censor media. The failure to recognize this leads to much confusion and controversy in debates about media content and policy.

- **There is a trade-off between complexity and convenience for both tools and ratings:**
Some critics argue parental control tools need to be more sophisticated; others claim parents can't understand the ones already at their disposal. But there is no magical "Goldilocks" formula for getting it "just right." There will *always* be a trade-off between sophistication and simplicity; between intricacy and ease-of-use.
- **Not all homes need parental control tools:** While blocking technologies or other parental control tools can be very useful for those households in which children are present, not all homes have children in them. In fact, less than 32% do. Moreover, the children in many of those households are below or above the ages when parental control tools may be necessary. [see Section II]
- **The role of household media rules and methods is underappreciated and those rules have an important bearing on this debate:** Surveys reveal that almost all parents use some combination of household media rules to control their children's media consumption. These household media rules include: (1) "where" rules (assigning a place for media consumption); (2) "when and how much" rules (creating a media allowance); (3) "under what conditions" rules (carrot-and-stick incentives); and, (4) "what" rules (specifying the programming kids can and cannot watch). Many households reject technical blocking tools in favor of these household media rules; others simply shun certain media and communications technologies altogether. This is another reason why the universe of homes that use or even need parental controls is smaller than most policymakers imagine. [see Section VI]
- **Mandatory defaults or restrictive settings will back-fire:** Mandating parental controls or restrictive default settings will back-fire. It is the equivalent of shipping products to market

in a “crippled” state and it will lead to consumer confusion, complaints, and increased efforts to “crack” or circumvent those controls. Black market devices would also become more prevalent. There are also many legal issues associated with using existing industry ratings or controls as a trigger for legal liability. [see Section IV]

- **The search for technological silver-bullets and “universal” solutions represents a quixotic, Holy Grail-like quest and it will destroy innovation in this space:** While we do not have a “universal” ratings system across all media—television, movies, music, video games, the Internet—current voluntary content rating systems *are* universal, or nearly universal, within their respective sectors. The same cannot be said of current “independent” ratings schemes, which—although they provide parents with beneficial information—fall short of being as comprehensive as industry-based ratings. And proposals to mandate “universal” controls and ratings across all media platforms would potentially destroy innovation in this space by substituting a government-approved, “one-size-fits-all” standard for the “let-a-thousand-flowers-bloom” approach, which offers diverse tools for a diverse citizenry. Finally, a universal ratings mandate would raise profound First Amendment concerns since it could constitute prior restraint and compelled speech. [see Section IV]
- **Media and technological convergence presents unique challenges:** An age of abundant, ubiquitously available media creates unique challenges. No one saw user-generated content and social networking capabilities coming ten years ago. “Blocking” technologies aren’t going to help as much here. Instead, sensible site self-policing, targeted intervention strategies, abuse reporting processes, and the possibility of “peer reporting” represent the best path forward.

- **Parental controls work best as part of a “layered approach” to dealing with objectionable content or communications:** Parental control tools and methods will not always provide perfect protection, but they can act as training wheels or speed bumps along the paths that children seek to go down. But technological controls are no substitute for education, mentoring, and good parenting practices. The best answer to the problem of unwanted media exposure or contact with others is for parents to rely on a mix of technological controls, informal household media rules, and, most importantly, education and media literacy efforts. Government can play an important role by helping educate and empower parents and children to help prepare them for our new media environment. In other words, a “layered approach” works best.
- **“Household standards” should trump “community standards”:** The ideal state of affairs would be a nation of fully empowered parents who have the ability to perfectly tailor their family’s media consumption habits to their specific values and preferences. Giving parents more information and tools so they can make media consumption decisions at the household level allows us to move away from the hopelessly ambiguous notion of “community standards”-based regulation and toward a world in which “household standards” become the new norm. In other words, each family decides for themselves; government officials need not decide for them. (see Section IX)
- **The Commission should tread cautiously in this proceeding in light of limited jurisdiction and First Amendment values in play here:** Finally, the Commission’s role in this matter is proscribed by two factors: jurisdiction and the First Amendment. The Commission has no authority over video games or virtual worlds, online video distribution networks or video hosting sites, mobile web content, MP3 players or iPods, P2P networks, VCRs or DVD

players, PVRs or TiVo, Internet filters, safe search tools, laptops, and so on. And yet, all these things (and much more) are mentioned in the Commission's *Notice*. Does the Commission recognize any boundaries to the oversight authority it asserts in the name of investigating "advanced blocking technologies"? It certainly should. One might argue that merely *studying* the marketplace poses no harm, but if the Commission were to go beyond mere studying and assert its regulatory powers, it could—and likely would—run afoul of the First Amendment's prohibition against meddling (even indirectly) with free speech and artistic expression. [see Section IX]

In light of these factors, the Commission's role in this proceeding should be limited to:

- Expanding information and education about existing tools and rating systems;
- Examining new or independent tools and ratings systems that parents might find useful (but not mandating them or tipping the balance against existing tools or rating systems); and
- Encouraging parents to use these tools and methods and to talk to their children about appropriate media use.

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Child Safe Viewing Act;)	
Examination of Parental Control Technologies for)	MB Docket No. 09-26
Video or Audio Programming)	
)	

**COMMENTS OF ADAM THIERER,
SENIOR FELLOW WITH THE PROGRESS & FREEDOM FOUNDATION (“PFF”)
AND THE DIRECTOR OF PFF’S CENTER FOR DIGITAL MEDIA FREEDOM**

Adam Thierer, Senior Fellow with The Progress & Freedom Foundation (“PFF”) and the director of PFF’s Center for Digital Media Freedom,¹ hereby offers comments in response to the Public Notice in the above-captioned matter, *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming*.

Much of what follows is taken from my PFF Special Report, *Parental Controls & Online Child Protection: A Survey of Tools and Methods*.² That report is updated frequently to take into account the rapidly-evolving marketplace for parental control tools and methods.

¹ The views expressed herein by the author are entirely his own and are not necessarily the views of the PFF board, fellows or staff.

² Adam Thierer, *Parental Controls and Online Child Protection: A Survey of Tools and Methods* (Washington, DC: The Progress & Freedom Foundation, Version 3.1, 2008), www.pff.org/parentalcontrols

I. INTRODUCTION: UNDERSTANDING THE ROLE AND LIMITS OF PARENTAL CONTROLS

This filing will show that the market for parental control technologies is functioning well and serving the needs of a diverse citizenry. Parental controls will be defined broadly to include *any tool or method that parents, guardians or schools might use to restrict or tailor the media content that children consume*. The “restrict or tailor” qualifier is important. Too often, parental controls are viewed as being merely restrictive in character. That is, they are used to block or filter media content. That is certainly one important use for parental controls; perhaps even the most important use for many families. But content *tailoring* is an equally important part of the parental controls mix.

Content tailoring refers to parents’ use of any tool or method that *enables* their families to see, hear, or consume content they would regard as “better” (*i.e.*, more educational, enriching, or ethical) for them. This is perhaps the most exciting part of the parental controls story today. Parental control tools and methods exist now that make it easier than ever before to tailor media content and consumption to a family’s specific needs and desires.

Some important caveats about parental controls are in order before exploring the marketplace for tools, ratings, and other methods of blocking and controlling content and communications.

A. No System is Foolproof and This is Not an Exact Science

The first caveat to keep in mind is that no rating system is perfect and no parental control tool is foolproof. Many critics are fond of pointing to supposed deficiencies in certain rating systems or technological controls and then attempt to use those problems to indict all voluntary ratings or private controls. But ratings and parental control tools need not be perfect to be preferable to government regulation.

Consider ratings first. What critics consistently forget—or perhaps intentionally ignore—is that media rating and content-labeling efforts are not an exact science; they are fundamentally subjective exercises. Ratings are based on value judgments made by humans who all have somewhat different values. Those doing the rating are being asked to evaluate artistic expression and assign labels to it that provide the rest of us with some rough proxies about what is in that particular piece of art, or what age group should (or should not) be consuming it. In a sense, therefore, all rating systems will be inherently “flawed” since humans have different perspectives and values that they will use to label or classify content.

Moreover, as Drs. Lawrence Kutner and Cheryl K. Olson, cofounders and directors of the Harvard Medical School Center for Mental Health and Media, note in their book *Grand Theft Childhood: The Surprising Truth about Violent Video Games*, “No [rating] system will ever be able to scrutinize and label all potentially offensive or upsetting content. The more complicated a system becomes, the less likely busy parents are to understand it and to actually use it.”³ Indeed, there will *always* be a trade-off between sophistication and simplicity; between intricacy and ease-of-use. And the growth of user-generated content will exacerbate this problem in coming years and necessitate creative solutions.

Likewise, technological controls will always be hindered by certain inherent limitations. Technologies, markets, and artistic expression all evolve, and they do so at an increasingly rapid pace in our modern Information Age. Moreover, controls can be cracked or circumvented.

³ Lawrence Kutner and Cheryl K. Olson, *Grand Theft Childhood: The Surprising Truth about Violent Video Games* (New York: Simon & Schuster, 2008), p. 186.

There's always someone out there—including, all too often, our own children—who are looking to evade technological controls.⁴

B. There Is No Reason to Believe that a Government-Mandated Solution Would Be Preferable to Private Controls

For these reasons, there will always be some critics who will argue that someone—presumably themselves or the government—can devise better ratings or controls. But, even setting aside the clear First Amendment concerns it would raise, there is no reason to believe that the government could actually do a better job.

If the government were responsible for assigning content ratings or labels, for example, the Commission or some other regulatory agency would simply substitute their own values for those of the voluntary rating boards or other labeling organizations in existence today. And the argument that government would provide more objective ratings or effective controls is also undermined by the grim reality of special-interest politics. Government officials would be more susceptible to various interest group pressures as they were repeatedly lobbied to change ratings or restrict content based on widely varying objectives and values. Inevitably, as has been the case with the broadcast indecency complaint process in recent years, a handful of particularly vociferous groups could gain undue influence over content decisions.⁵ That possible outcome raises what the Supreme Court has referred to as the “heckler’s veto” problem since a vocal minority’s preferences could trump those of the public at large.⁶

⁴ Tom A. Peter, “Internet Filters Block Porn, But Not Savvy Kids,” *Christian Science Monitor*, April 11, 2007, www.csmonitor.com/2007/0411/p13s02-lihc.htm

⁵ Adam Thierer, “Examining the FCC’s Complaint-Driven Broadcast Indecency Enforcement Process,” Progress & Freedom Foundation *Progress on Point* 12.22, November 2005, www.pff.org/issues-pubs/pops/pop12.22indecencyenforcement.pdf

⁶ *Reno v. ACLU*, 521 U.S. 844, 880 (1997).

With private, independent rating and labeling systems, by contrast, those assigning ratings or labels are intentionally isolated from lobbying or other interest group pressures. This is what makes the argument for “transparency” in rating systems so disingenuous, or even somewhat dangerous. If “transparency” means forcing raters to be exposed to endless special-interest lobbying or other pressures, one wonders if that would really produce a better system. Indeed, such “transparency” would more likely produce a system that bowed to those pressures. For example, if those assigning video game ratings were not anonymous, they might be harassed by both game developers (who want to make them more lax) and game critics (who want to make them more stringent).⁷ This does not mean the raters ignore public input. To the contrary, private rating boards and labeling bodies poll the public and monitor what critics are saying to adjust their ratings accordingly. But if the government forced their ratings systems to be open to all who cared to provide input (including the public policymakers themselves), it would result in a circus-like atmosphere and little content would get rated in a timely manner.⁸

Similarly, there is no reason to believe the government could construct more rigorous parental controls or screening technologies. Consider Internet filters, for example. Starting with the passage of the Communications Decency Act of 1996, there have been endless political

⁷ Adam Thierer, “Can Government Improve Video Game Ratings?” Progress & Freedom Foundation, *PFF Blog*, October 26, 2006, http://blog.pff.org/archives/2006/10/can_government.html

⁸ As Competitive Enterprise Institute analysts Cord Blomquist and Eli Lehrer argue, “A federally mandated video game rating system would require committee hearings, committee mark-up sessions, and floor debate. At the end of this process a new federal regulatory agency would exist, or an existing agency’s powers would be expanded. Proposed changes in the system could require Congress to act, starting the legislative process anew. By contrast, the ESRB can respond swiftly to developments in the industry that require any adjustment in the ratings system.” Cord Blomquist and Eli Lehrer, “Politically Determined Entertainment Ratings and How to Avoid Them,” Competitive Enterprise Institute *Issue Analysis* 2007 No. 12, December 2007, p. 22, <http://cei.org/pdf/6292.pdf>

debates about the efficacy of private filters relative to government content controls. Policymakers typically argue that regulation is needed because filters are not 100% effective in blocking pornography or other types of objectionable online content.

No doubt this point is true, but what of it? During a recent trial about the merits of the Child Online Protection Act (COPA) of 1998, the Department of Justice (DOJ) introduced evidence showing that major filters blocked sexually explicit content 87.4 to 98.6% of the time,⁹ and the judge in the case concluded that filters generally block an average of 95% of sexually explicit material.¹⁰ The DOJ seemed to suggest that this was not good enough, but would government regulation really produce a better track record than that? It's doubtful, especially because the government is largely powerless to control offshore activity. Private filters, by contrast, can capture objectionable offshore material. Private filters can also use industry standard identification systems to allow legitimate rated commercial content to be seen while screening out unknown or unrated content. And new methods are being developed and deployed to monitor and identify content, such as image-recognition technologies, which can further facilitate screening and filtering.

C. The Goal Should Be 'Let-a-Thousand-Flowers-Bloom,' Not 'One-Size-Fits All'

Moreover, it is reasonable to assume that a market of commercial filters and other technological controls will flourish if governments promote industry experimentation rather than imposing a "one-size-fits-all" regulatory model. A marketplace of controls and filters can then develop that is more closely tailored to the diverse values of the citizenry. Government

⁹ For a breakdown of how successful various filters were, see www.aclu.org/freespeech/internet/27490res20061120.html

¹⁰ *American Civil Liberties Union v. Gonzales*, No. 98-5591 (U.S. District Court, Eastern District of Pennsylvania, March 22, 2007), p. 35, www.cdt.org/speech/copa/20070322copa.pdf.

controls, by contrast, essentially treat all households as having the same needs and values, which we know is not the case. Even though not all private controls will be equally effective, failure will be detected more rapidly and the better systems will gradually win out as more and more legitimate content is tagged and rated.

D. Thinking in Terms of Training Wheels and Speed Bumps

Instead of thinking of ratings and blocking controls as absolute controls, it makes more sense to think of them in terms of training wheels and speed bumps. If we want to make our kids slow down and be more cautious on today's "information highways," we can add more speed bumps and affix better training wheels on their bikes. But even with training wheels, kids will still fall off their bikes sometimes. And long after they learn how to ride without training wheels and have given up their bikes for cars, speed bumps can only slow them down so much; they won't stop them from speeding entirely.¹¹

What do we do about it as parents and a society? We promote better industry-wide safety designs, we add layers of protection, and we try to educate our children about the dangers they face. When they are young and still riding bikes, we make them wear helmets, warn them of the dangers of traffic, and tell them to slow down. And when they become teenagers and get their first car, we make them wear their seat belts and avoid aggressive driving, and we still keep telling them to slow down! In sum, *we use the protections and safeguards at our disposal while educating them about safe and responsible use.*

¹¹ Nancy E. Willard, author of *Cyber-Safe Kids, Cyber-Savvy Teens*, argues that "Placing significant reliance on parental controls may end up backfiring, because such reliance often leads to false security. ... The biggest problem with the promotion of protection technologies is that these technologies will never be totally effective." Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy Teens* (San Francisco, CA: Jossey-Bass, 2007), p. 31, 33-4.

This is the same mindset we need to adopt when it comes to parental controls and online child safety.

II. ACCESSING THE RELEVANT UNIVERSE OF PARENTAL CONTROL USERS

Another important caveat about parental controls relates to how many homes actually need them.¹² Simply put, not every U.S. household needs parental controls. Indeed, the number of families that might need or want these tools is smaller than most think. The percentage of homes that might need parental control technologies is certainly no greater than the 32% of U.S. households with children in them. Moreover, the relevant universe of potential parental control users is likely much less than that because households with very young children or older teens often have little need for parental control technologies. Finally, some households do not utilize parental control technologies because they rely on alternative methods of controlling media content and access in the home, such as household media rules. Consequently, policymakers should not premise regulatory proposals upon the limited overall “take-up” rate for parental control tools since only a small percentage of homes might actually need or want them.

To better understand why this is the case, consider an analogy. Imagine a survey or study that gauged the efficacy of protective child cabinet locks by asking whether *all* U.S. household employed such safety measures on kitchen and bathroom cabinets. Such a survey would yield truly absurd results. The vast majority of Americans have no need for baby locks because either: (a) they have no children present in the home, (b) their children are of an age

¹² This section is condensed from: Adam Thierer, “Who Needs Parental Controls? Assessing the Relevant Market for Parental Control Technologies,” Progress & Freedom Foundation, *Progress on Point* 16.5, February 27, 2009, www.pff.org/issues-pubs/pops/2009/pop16.5parentalcontrolsmarket.pdf

where such locks are not needed, or (c) they take other steps to protect their children from harmful products that might be in the home. Thus, any survey or study that evaluated the success of child safety cabinet locks in terms of adoption rates by using *all* households as the relevant universe of analysis would produce highly skewed, inaccurate results. Such a survey or study would conclude that few households use such controls and, therefore, those controls are a failure, even though that is an illogical conclusion based on a faulty statistical method.

Regrettably, a similar statistical fallacy plagues discussions about parental control technologies today.¹³ Only a small percentage of households need parental controls, yet many surveys or critiques of parental control technologies suffer from similar statistical flaws by over-estimating the relevant universe of households.

A. Calculating How Many Homes Have Children Present

A more accurate methodological approach to studying this issue can be conducted using U.S. Census Bureau data to determine which households have children and might need to employ parental control technologies. According to the Census Bureau's *Statistical Abstract of the United States*, as of 2007, over 68% of American homes did *not* have any children under 18 years of age in residence.¹⁴ (Stated differently, only 32% of U.S. households have children in them). This percentage is calculated as follows:

¹³ Adam Thierer, "Distorting Numbers in the Debate over Parental Controls," Progress & Freedom Foundation, *PFF Blog*, March 26, 2007, http://blog.pff.org/archives/2007/03/distorting_numb.html

¹⁴ U.S. Census Bureau, *2008 Statistical Abstract of the United States*, Table No. 58, available at www.census.gov/compendia/statab/tables/09s0058.pdf

Exhibit 1:
Formula for Calculating the Percentage of Households without Children

$$\begin{aligned} & \text{Nonfamily Households} + \text{Family Households without own Children}^{15} \\ & \div \\ & \text{Total Households} \\ & = \\ & \text{\% of Households without Children} \end{aligned}$$

Thus, using recent Census Bureau data, the percentage of homes without children for 2007, the most recent year for which data is available, can be computed as follows:

Exhibit 2: Households without Children Calculation for 2007

$$\begin{aligned} & 37,587 + 41,668 \\ & \div \\ & 116,011 \\ & = \\ & 68.3\% \end{aligned}$$

Incidentally, the number of homes without children in them has been steadily rising for many years. The adjoining exhibits present a breakdown of the Census Bureau data for select years from 1960 to the present.

Exhibit 3: Breakdown of U.S. Households With and Without Children

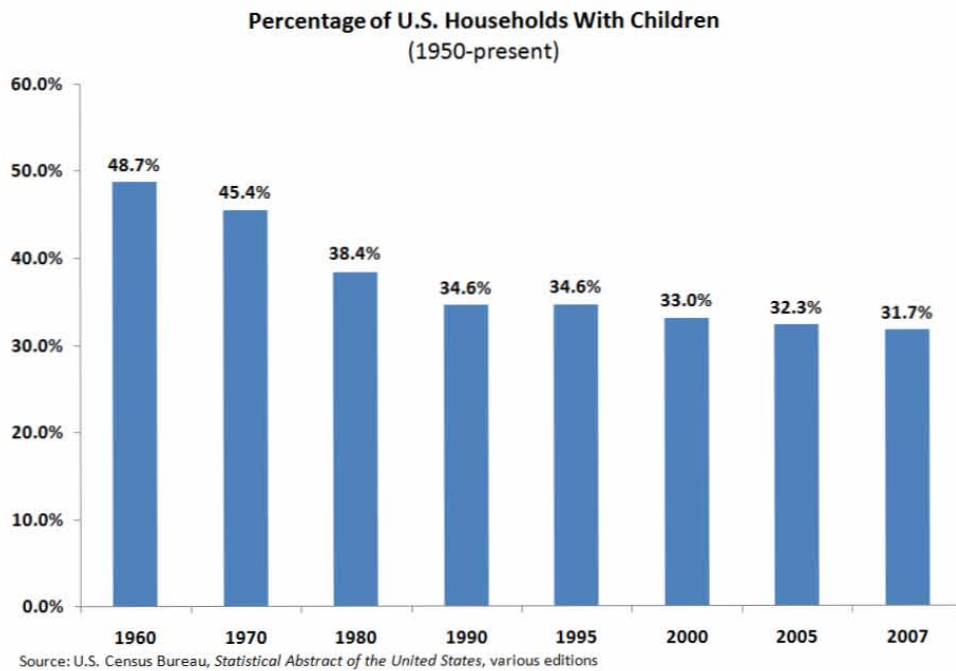
	1960	1970	1980	1990	1995	2000	2005	2007
Total Households (in thousands)	52,799	63,401	80,776	93,347	98,990	104,705	113,146	116,011
Nonfamily Households	7,895	11,945	21,226	27,257	29,686	32,680	36,136	37,587
Family Households With Own Children	25,690	28,812	31,022	32,289	34,296	34,605	36,520	36,757
Family Households Without Own Children	19,215	22,774	28,528	33,801	35,009	37,420	40,491	41,668
Total Households Without Children	27,110	34,719	49,754	61,058	64,695	70,100	76,627	79,255
% of Households Without Children	51.3%	54.8%	61.6%	65.4%	65.4%	67.0%	67.7%	68.3%
% of Households With Children	48.7%	45.4%	38.4%	34.6%	34.6%	33.0%	32.3%	31.7%

Source: U.S. Census Bureau, *Statistical Abstract of the United States*, various years

¹⁵

According the Census Bureau, a *nonfamily household* “can be either a person living alone or a householder who shares the housing unit only with his or her nonrelatives—for example, boarders or roommates.” A *family household* “has at least two members related by birth, marriage, or adoption, one of whom is the householder. Family households are maintained by married couples or by a man or woman living with other relatives—children may or may not be present.” Obviously, the relevant subset of those family households for this analysis would be those without any children present. See U.S. Census Bureau, “America’s Families and Living Arrangements: 2003,” November 2004, p. 2, www.census.gov/prod/2004pubs/p20-553.pdf

**Exhibit 4:
Steady Decline of Homes With Children Present**



This makes it clear why it is illogical to survey *all* homes about parental control usage. It is highly unlikely adult-only homes would be using parental controls or blocking services when they have the ability to block objectionable content and communications in other ways.¹⁶ Thus, the relevant universe of homes that should be considered when evaluating parental control technologies' usage would only be those 32% of U.S. households with children present.

B. Homes with Very Young or Much Older Children Have Less Need for Controls

The actual relevant universe of homes, however, is likely much smaller than the 32% of homes with children present. Even in those homes with children in residence, most of those

¹⁶ Of course, some adult-only households with heightened sensitivities about certain types of programming might use some blocking or filtering tools to keep unwanted content or communications out of the home. It seems more likely, however, that those households would simply avoid such material by choosing not to subscribe to certain services or just changing channels and only visiting certain trusted websites.

families will not need to use parental control technologies for children under a certain age (say 5 or 6 years) or older than a certain age (perhaps 15 or 16).

For example, many parents tightly control their children's media consumption habits before they reach a certain age. Before the age of six, for example, parents can (and do) employ a wide variety of household rules and methods to control media and communications in the home. As will be shown in Section VI, household media rules that often serve as a substitute for parental control technologies.

Likewise, after children reach a certain age—especially as they get closer to leaving home—the training wheels come off, so to speak, and parents begin to trust their children to make more media decisions on their own. Or, better yet, parents talk to their kids about objectionable content and communications, but likely without rigid parental control technologies in place. Many parents of teenage children also use various household media rules, especially “carrot-and-stick” incentives, to encourage them to use media and online connections in a wise (or limited) fashion.

Some policymakers have acknowledged these realities. For example, in August 2007, Rep. Ed Markey (D-Mass.), former chairman of the House Telecommunications & Internet Subcommittee, was asked by *Broadcasting & Cable* if existing TV ratings and the V-Chip were effective or needed tweaking. In response, Markey noted:

The evidence is that parents who have small children and know about the V-chip use it at relatively high levels and like it. Obviously, most families aren't in that situation, meaning that they don't have small children. So it's not something that every person is going to be talking about because it would never occur to them to use a V-chip in 85% or 90% of all homes. *So it's in that subset of homes* that, among the parents who know about it, there is a very high degree of satisfaction.¹⁷

Rep. Markey is correct that those homes with much older children would likely not need to utilize the V-Chip, but it's also just as true for those households with very young children, for the reasons stated above.

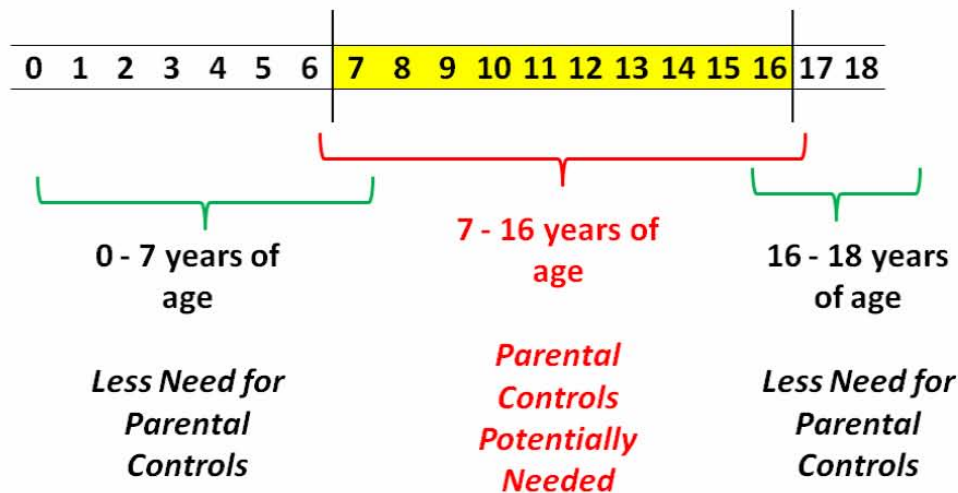
Putting these two pieces of information together, the adjoining exhibit depicts when it is most likely that parental control technologies will be used in the home (for those homes in which children are present). If anything, this estimate (at least for teens) may be a bit conservative since the window when parental controls may be relevant could be even narrower for many families.

¹⁷ Quoted in John Eggerton, *Broadcasting & Cable*, "Ed Markey on TV Violence, Media Ownership and the Digital Transition," August 20, 2007, [emphasis added]
www.broadcastingcable.com/article/CA6470038.html?display=Breaking+News&referral=SUPP&nid=2228

Exhibit 5: Ages When Parental Controls Most Likely Needed

When are Parental Controls Needed?

Ages 7 to 16 are Likely Years When
Parental Controls are Employed in Most Homes



Source: Adam Thierer, Progress & Freedom Foundation

C. For a Variety of Reasons, Some Families Opt to Never Use Parental Controls

Another important consideration is that, for whatever reason, some parents rarely, or never, employ parental control technologies in the home, even when their kids are in the age band where those technologies would be most helpful. A significant, but unknown, number of parents reject parental control technologies for a combination of the following reasons:

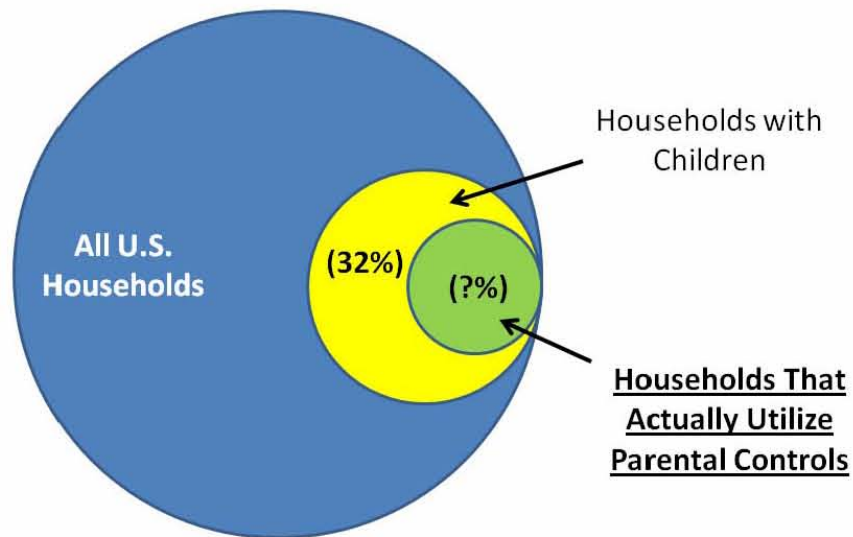
- They have an aversion to parental control technologies, perhaps fearing it creates distrust between them and their kids;
- They don't think parental control technologies work;
- They believe their own household media rules and restrictions (see Section VI) constitute a more sensible approach;
- They feel comfortable making their own judgments after consulting ratings, program guides, and other information provided by media providers or third party media watchdog or rating organizations (see Section VII);
- They just don't allow many media or communications devices in the home;
- Or perhaps some of them are too busy (or just lazy!)

The fact is, every family is different, with unique values and preferences regarding media consumption and interactive communications. But there mere fact that some households choose not to use parental control technologies does not necessarily mean they are not taking other steps to control media, monitor communications, or mentor their children.

Exhibit 6: The Big Picture

Who Needs Parental Controls?

Far Less than 32% of U.S. Households Likely Need to Parental Controls



Source: Adam Thierer, Progress & Freedom Foundation

D. The Big Picture: Only a Small Percentage of Homes Need Parental Controls

Recognizing that every family is different and will bring different needs, values, and approaches to the task of raising children, the adjoining exhibit depicts just how narrow of a slice of the overall universe of U.S. households actually needs parental control technologies. In essence, only a small subset of the subset of homes with children present will ever need parental control technologies.

While we know with certainty the percentage of that first subset—32%—there is no way to accurately measure the second “subset of the subset” of homes. But I believe it is reasonable to assume that of those 32% of homes with children present, at least half of them have little

need for parental control technologies. The many other factors identified above mean that many of those 32% of homes with children will forgo, or have no need for, parental control technologies.

III. A SURVEY OF THE MARKETPLACE FOR PARENTAL CONTROL TOOLS AND RATING SYSTEMS

This section provides a comprehensive overview of the parental controls and rating systems on the market today. Each major media sector will be described separately.

A. Television

Television programming remains the focus of more public policy debates than any other type of media content. That is not surprising given the continued centrality of television as a mass medium and cultural phenomenon in our society. Even as consumption of other types of content increases, television still dominates. Luckily, numerous tools and methods exist by which parents can restrict consumption of objectionable television programming in the home and tailor the video programming their children see on their various media devices.

1. The V-Chip and TV Ratings

As a standard feature in all televisions 13 inches and larger built after January 2000, the V-Chip gives households the ability to screen televised content by ratings that are affixed to almost all programs.¹⁸ The V-Chip can be accessed through the setup menus on televisions, or is often just one click away using a designated button on the TV's remote. Households can then

¹⁸ It is important to realize that most video consumed on televisions today is not from traditional broadcast stations. New video distribution sources such as cable, satellite, DVD, Blu-Ray, and IPTV all inherit a social norm and cultural responsibility to allow parents controls that are easy to set once and enforce everywhere.

use password-protected blocking to filter programs by rating. The rating system, available online at www.tvguidelines.org/ratings.htm, offers seven age-based designations:

Exhibit 7: TV Ratings



All Children

Directed to Children Age 7 and Older

Directed to Older Children Due to Fantasy Violence

General Audience

Parental Guidance Suggested

Parents Strongly Cautioned

Mature Audience Only

The TV rating system also uses several content descriptors to better inform parents and all viewers of the nature of the content they will be experiencing.

Exhibit 8: TV Content Descriptors¹⁹

D	Suggestive Dialogue
L	Coarse Language
S	Sexual Situations
V	Violence
FV	Fantasy Violence

These age-based ratings and content descriptors appear in the upper left hand corner of the screen at the start of each television program. If the program is more than one hour, the icon will reappear at the beginning of the second hour. (For some programs, the ratings appear after every commercial break). The ratings and descriptors also appear on the TV's on-screen menus and interactive guides, on the TV networks' websites, and in local newspaper or *TV Guide* listings. This information is also encoded and embedded into each TV program so that the V-Chip or other devices can screen and filter by ratings.

The Federal Communications Commission also hosts a website that provides detailed instruction on how to use the V-Chip.²⁰ "TV Watch," a coalition of media experts and media organizations, provides a website with tutorials and tool kits to help parents program the V-Chip and find other tools to control television in the home.²¹ In September 2008, TV Watch

¹⁹ The meaning of the content descriptors varies depending on the age-based rating to which they are attached. For example, "L" means "infrequent coarse language" when attached to a TV-PG rating and "strong, coarse language" when attached to a TV-14 rating. See www.tvguidelines.org/ratings.asp

²⁰ www.fcc.gov/vchip

²¹ www.televisionwatch.org

launched a useful “Television Tools for Parents 101” guide to help explain ratings and technical television blocking controls.²² And a new industry sponsored campaign entitled “The TV Boss”²³ offers easy-to-understand tutorials explaining how to program the V-Chip or cable and satellite set-top box controls. As part of the effort, several public service announcements (PSAs) and other advertisements have aired or been published reminding parents that these capabilities are at their disposal.

Exhibit 9: “TheTVBoss.org” Website



Importantly, the relatively low V-Chip usage rates among U.S. households should not be used as an excuse for government regulation of television programming. To reiterate what was noted above, some polls or surveys of V-Chip and parental control usage unfairly include *all* households in the sample group, which means they are including in their results the millions of

²² “Television Tools for Parents 101,” TV Watch, September 2008, www.televisionwatch.org/HelpForParents/toolsforparents.pdf

²³ www.thetvboss.org

households without children in them that have no incentive to use the V-Chip or any other parental control technologies.²⁴ And because most American homes do not have any children under 18 years of age in residence, it means the universe of V-Chip users is smaller than most people realize. (See Section II) Moreover, the other caveats discussed in this filing also apply here regarding the many homes that forgo any parental controls because they instead rely on informal household media rules. (See Section VI) Or, even those homes with children in residence will not all need to use parental control technologies before a certain age or after a certain age because parents feel there are better approaches for those age groups.

Finally, as discussed below, the vast majority of American homes now rely on many alternative technologies and methods to filter or block unwanted programming. Many families will forgo V-Chip capabilities in light of the alternative technological controls at their disposal. A November 2005 survey by the polling firm Russell Research revealed that twice as many parents frequently use the parental controls that offered by their cable and satellite providers as use the V-Chip controls built into their television sets.²⁵ In other words, the V-Chip is just one of many tools or strategies that households can use to control television programming in their homes.

²⁴ Adam Thierer, "Distorting Numbers in the Debate over Parental Controls," Progress & Freedom Foundation, *PFF Blog*, March 26, 2007, http://blog.pff.org/archives/2007/03/distorting_numb.html

²⁵ "Survey: Parents Combine Old-Fashioned TV Rules and Latest Blocking Technologies to Manage Kids' TV," TV Watch *Press Release*, November 28, 2005, www.televisionwatch.org/NewsPolls/PressReleases/PR008.html

2. Cable and Satellite TV Controls

With roughly 86% of U.S. households subscribing to cable or satellite television systems,²⁶ the tools that multichannel video providers (cable, satellite, and telephone companies) offer to subscribers are a vital part of the parental controls mix today. Parental controls are usually just one button-click away on most cable and satellite remote controls and boxes.

Both analog and digital boxes allow parents to block individual channels and lock them with passwords so that children can't access them. Newer, digital boxes offer more extensive filtering capabilities that allow programs to be blocked by rating, channel, or title. Some systems even allow users to block the program descriptions on the interactive guide (for adult pay-per-view programming, for example) if families do not want them to be visible.

Those cable subscribers without digital set-top boxes can request that cable companies take steps to block specific channels for them. A comprehensive survey of the content controls that cable television providers make available to their subscribers can be found on the National Cable and Telecommunications Association's (NCTA) "Control Your TV" website.²⁷

²⁶ Federal Communications Commission, *Twelfth Annual Video Competition Report*, February 10, 2006, p. 118, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-11A1.pdf

²⁷ <http://controlyourtv.org>

Exhibit 10:

NCTA's "ControlYourTV.org" Website

HOME | FAQ | SITE MAP | FOR MEDIA | EMAIL UPDATES

Versión en Español



Take control. It's easy.

The cable industry has a longstanding commitment to addressing parents' concerns about what they and their children see on television. Cable operators and program networks are strongly committed to addressing these concerns. Cable's approach to addressing indecency and violence on television is based on the concepts of [Control](#), [Choice](#) and [Education](#).

NEW: [Watch a video on using parental controls.](#)

Personalized Help

[Click here](#) to request personalized instructions on how to configure parental controls in your TV and Cable equipment. Also, [sign up today](#) for periodic updates and tips about managing TV viewing in your home.

Control

Take charge of your TV viewing through parental controls; they're easy to use and provide a powerful range of options. [Learn more . . .](#)



Choice

Your family can choose from cable's wide range of programming, which includes many shows perfect for kids and the whole family. [Learn more . . .](#)



Education

Want more info about becoming media smart? Help is available. [Learn more . . .](#)



Cable launches new Public Service Announcements about Parental Controls. [Watch the Video.](#)

Copyright Cable in the Classroom and The National Cable & Telecommunications Association.

Aftermarket solutions are also available that allow parents to block channels. The "TV Channel Blocker" gives households the ability to block any analog cable channel between channels 2 and 86, including broadcast stations carried by the cable operator.²⁸ Homeowners themselves can install the unit on the wall where the cable line enters the home. It can then block specific channels on any television in the home. The unit sells online for \$99.99.

Satellite providers DirecTV²⁹ and EchoStar's Dish Network³⁰ also offer extensive parental control tools via their set-top boxes. And telephone companies such as AT&T and

²⁸ www.tvchannelblocker.com

²⁹ www.directv.com/DTVAPP/global/contentPage.jsp?assetId=900007 and www.directv.com/DTVAPP/equipment/demoInfo.jsp?assetId=1100093

³⁰ www.dishnetworkproducts.com/products/parental_controls.php

Verizon are also getting into the video distribution business and offering similar tools. Many of the same set-top boxes deployed by the cable industry are also used by those telco providers. Therefore, the parental control capabilities are quite similar across both industries. (Incidentally, as the blending of the Internet and television continues with the rise of Internet protocol-based television delivery, there will be increased pressure for industry to rally around clear international standards for content identification and independent ratings. This should ensure that still more content gets rated/labeled.)

Some multichannel operators also offer subscribers the option of buying a bundle of “family-friendly” channels. For example, Dish Network offers a “Family Pak”³¹ and DirecTV offers a “Family Choice” bundle of channels.³² Many cable operators offer similar bundles, but parents must consult their local provider to get details since packages vary by zip code or county.³³ Major cable operators such as Comcast,³⁴ Time Warner,³⁵ Cox,³⁶ Insight Communications,³⁷ Mid-Continent,³⁸ and Bright House³⁹ all offer family packages. Also, a unique satellite service called Sky Angel offers over 70 channels of Christian and family-friendly

³¹ www.dishnetworkproducts.com/packages.php

³² www.directv.com/DTVAPP/packProg/channelChart1.jsp?assetId=1000005

³³ A good example from my home county of Fairfax, Virginia, is the Family Package that Cox Communications offers. See www.cox.com/fairfax/cable/familyservice.asp

³⁴ www.comcast.com/customers/faq/FaqCategory.ashx?CatId=356

³⁵ www.timewarnercable.com/corporate/programming/familychoice.html

³⁶ www.cox.com/fairfax/cable/familyservice.asp

³⁷ www.insight-com.com/documents/Insight_01172006.pdf

³⁸ www.midcocomm.com/resourcecenter/index.cfm/168/Cable/Digital-Family-Tier-Infomaiton

³⁹ http://cfl.mybighthouse.com/products_and_pricing/digital_cable/familypack.aspx

choice(s) that households can subscribe to if they want only religious programming to be available in their homes.⁴⁰

3. Other Technological Control Measures for Television

For those families that want to block out televised programming aired during certain hours of the day or limit how much TV can be viewed at all, technological tools exist that can make that possible. The Family Safe Media website sells a half dozen “TV time management” tools that allow parents to restrict the time of day or aggregate number of hours that children watch programming.⁴¹ Most of these devices, such as the “Bob TV Timer” by Hopscotch Technology⁴² and the “TV Allowance” television time manager,⁴³ feature PIN-activated security methods and tamper-proof lock boxes that make it impossible for children to unplug or reset the device. Parents can use these devices to establish a daily or weekly “allowance” of TV or game screen time and then let children determine how to allocate it. Similarly, “credit-based” devices such as the “Play Limit” box require children to place time tokens in a metallic lockbox to determine how much TV or game time is allowed.⁴⁴ Parents can provide a certain allowance of tokens to restrict the overall amount of screen time.

⁴⁰ www.skyangel.com

⁴¹ www.familysafemedia.com/tv_time_management_tools_-_par.html

⁴² www.hopscotchtechnology.com

⁴³ www.tvallowance.com

⁴⁴ www.playlimit.com

Exhibit 11: The “Weemote”



Another innovative technology to restrict children’s viewing options by children is the appropriately named the “Weemote.” It is a remote control made for children that has only a handful of large buttons. Parents can program each button to call up only those preset channels that they approve of for their children. No other channels can be accessed using the remote. The product has a suggested retail price of \$24.95.⁴⁵

For those families looking to take more direct steps to specifically curb potentially offensive language heard on some televised programs, solutions are available. For example, over seven million Americans currently use TVGuardian systems, which bill themselves as “The Foul Language Filter.” TVGuardian’s set-top boxes filter out profanity by monitoring the closed-caption signal embedded in the video signal and comparing each word against a dictionary of more than 150 offensive words and phrases. If the device finds a profanity in this broadcast, it temporarily mutes the audio signal and displays a less controversial rewording of the dialog in a closed-captioned box at the bottom of the screen.⁴⁶ The device can also be tailored to

⁴⁵ www.weemote.com

⁴⁶ www.tvguardian.com

individual family preferences to edit out references that some might consider religiously offensive.

4. Video Empowerment: VCRs, DVRs & VOD

One of the most important developments on the parental controls front in recent years has been the rapid spread of VCRs, DVD players, digital video recorders (DVRs), and video on demand (VOD) services. These technologies give parents the ability to accumulate libraries of preferred programming for their children and determine exactly when it will be viewed. Using these tools, parents can tailor programming to their specific needs and values.⁴⁷ If certain parents believed that their children should only be raised solely on reruns of *The Lone Ranger* and *Leave it to Beaver*, then these new media technologies can make it happen!

To use a personal example: My wife and I have developed a strategy of designating a specific television in our home for most of our children's media consumption and then using a DVR to amass a large library of programming we believe is educational, enriching, and appropriate for them. As a result, when we allow our children some TV time, we always know that the episodes of *Dora the Explorer*, *Go Diego Go*, *Blue's Clues*, and *The Wiggles* that we approve of for our kids will be available. Dozens of other programs can be cataloged and archived in this fashion and then supplemented with VHS tapes, DVDs, VOD downloads, and computer software. Needless to say, such content tailoring was not an option for families in the past.

⁴⁷ "[PVRs] are quickly revolutionizing the way families watch television, with easy-to-use systems and a convenience that every family can appreciate." Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), p. 172.

The following tools and technologies are helping to empower families to take more control over their video choices:

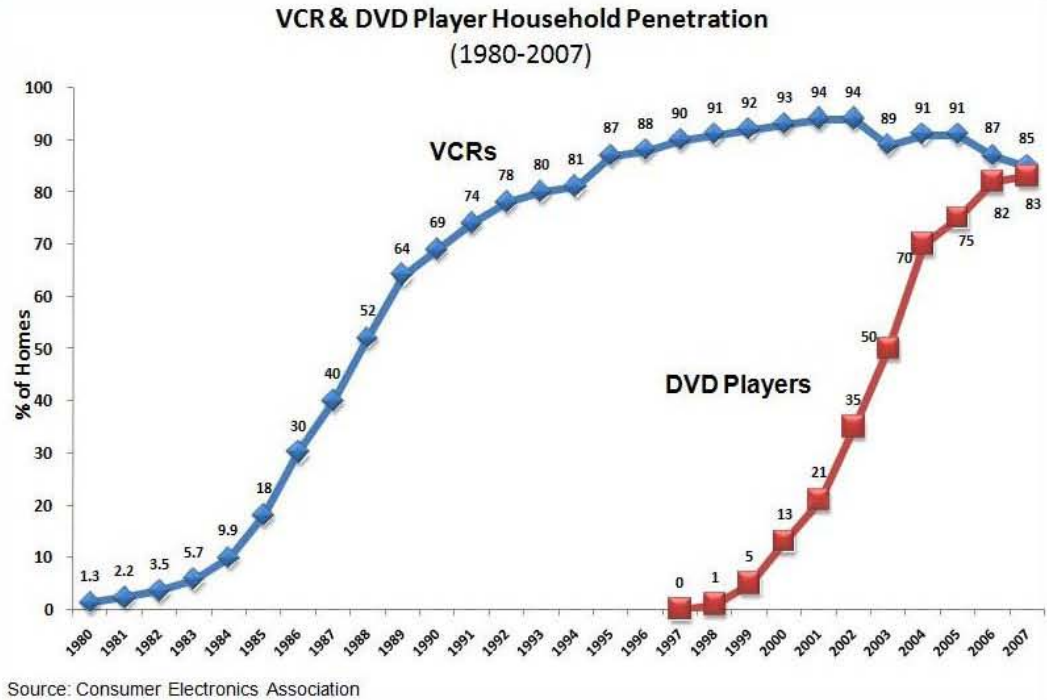
a) VCRs and DVD players / recorders

Many households continue to use video tapes and DVDs to build libraries of preferred programming. Parents can either purchase original copies of programs on VHS or DVD, or they can record shows when they appear on television on VHS tapes or recordable DVDs. The Consumer Electronics Association (CEA) estimates that 85% of U.S. households have at least one VCR. That is down from a high of 91% in 2005. The number of VCRs in homes is declining steadily because consumers have been replacing them with DVD players and DVD recorders. According to CEA, 83% of households have at least one DVD player, up from 13% in 2000. (Exhibit 13 documents the growth of VCR and DVD household penetration.)

Of course, as Larry Magid of CBS News.com points out, “VCRs are a hassle. You have to remember to program them, make sure you have a blank tape inserted, label and keep track of the recorded tapes, and insert them for the kids when they’re ready to watch.”⁴⁸ Much the same is true of DVD recorders. That is why the rise of the next-generation digital media devices described below is so important. Those devices help parents simplify and automate the content tailoring process in their homes.

⁴⁸ Larry Magid, “TV Tips for Parents,” *CBS News.com*, August 2, 2002, www.cbsnews.com/stories/2002/08/07/scitech/pcanswer/main517819.shtml

Exhibit 12: VCR & DVD Player Usage



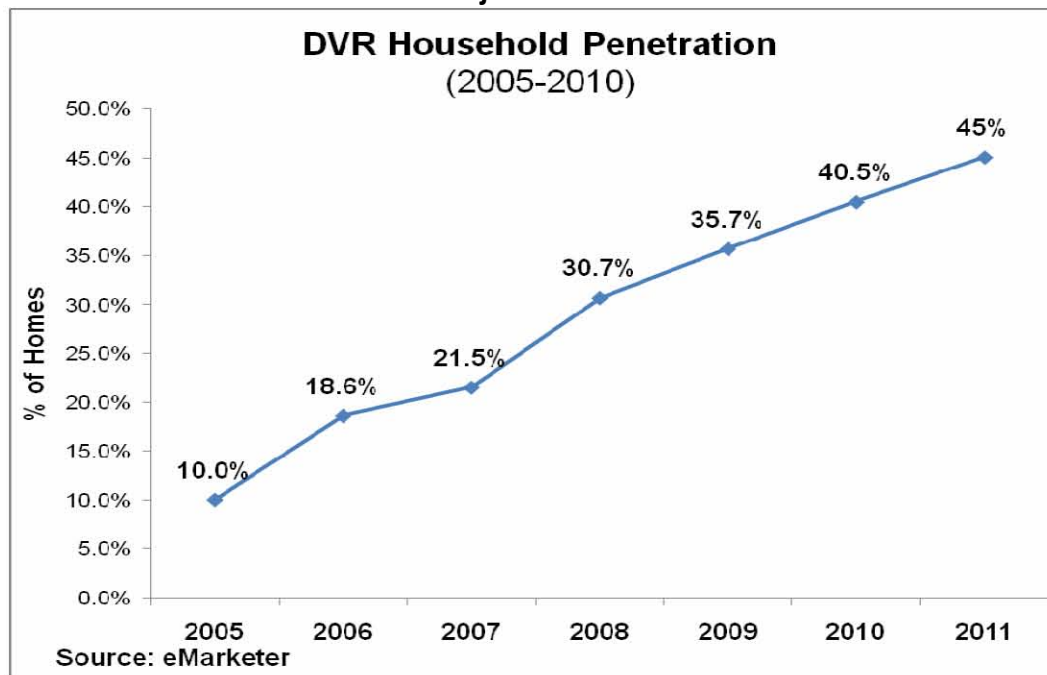
b) *Digital video recorders (DVRs) / Personal video recorders (PVRs)*

Considering the significant amount of buzz we hear about them today, it's easy to forget that digital video recorders (sometimes referred to as personal video recorders) are not even a decade old yet. But when TiVo and ReplayTV hit the market in 1999, it helped usher in what many regard as a revolution in television.⁴⁹ Those devices gave consumers an unprecedented level of control over their viewing experiences by allowing them to instantly pause, rewind, and fast-forward programming. DVRs also let consumers watch television on their terms by building an archive of desired programming. Today, all DVRs—including those sold or leased by cable, telco, and satellite operators—offer these features. Those tools and functions are particularly helpful to parents. “[DVRs] are quickly revolutionizing the way families watch television, with

⁴⁹ Glenn Derene, “The End of TV As We Know It,” *Popular Mechanics*, June 14, 2007, www.popularmechanics.com/blogs/technology_news/4217964.html

easy-to-use-systems and a convenience that every family can appreciate,” argues Sharon Miller Cindrich, author of *e-Parenting: Keeping Up with Your Tech-Savvy Kids*.⁵⁰

Exhibit 13: Projected Growth of DVRs



The DVR revolution is certain to continue and spread. Consider these facts and recent marketplace developments:

- “Consumers are beginning to embrace digital video recorders (DVRs) as they once did VCRs,” notes John P. Mello of the *E-Commerce Times*.⁵¹ Indeed, according to the Leichtman Research Group, a market research firm, more than one in every five U.S. households now have a digital video recorder, up from about one in every 13 households just two years ago.⁵² Leichtman Research also predicts that roughly 50% of all homes will have a DVR by 2011.⁵³

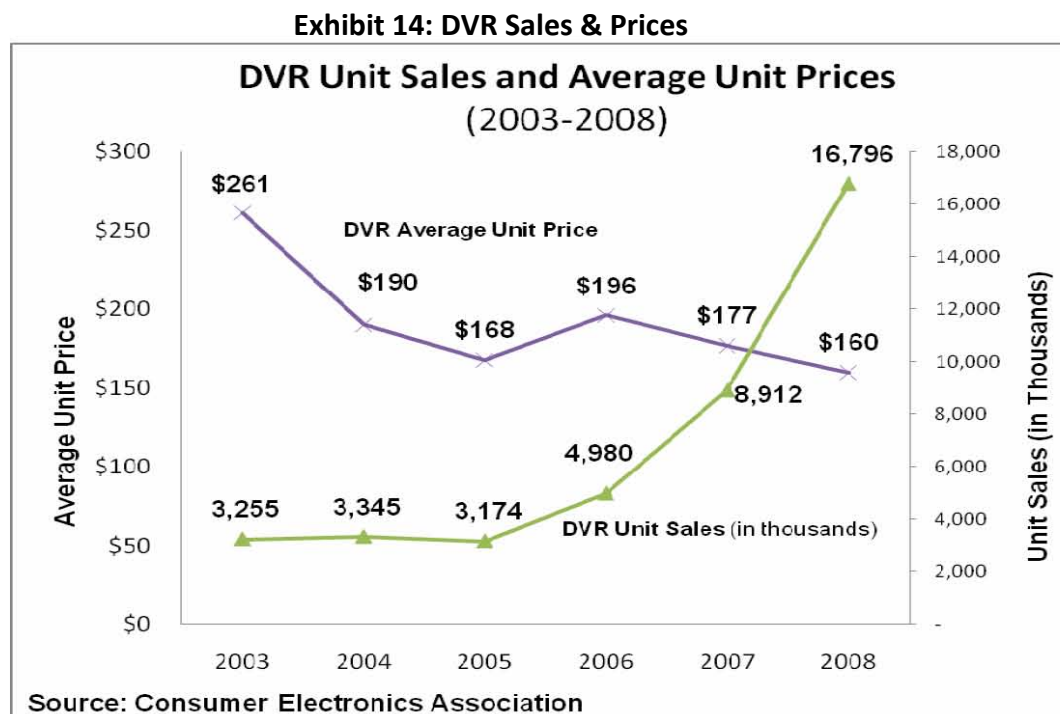
⁵⁰ Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), p. 172.

⁵¹ John P. Mello, “DVR Market Penetration: Riding a Provider-Powered Wave,” *E-Commerce Times*, September 26, 2007, www.ecommercetimes.com/story/trends/59497.html

⁵² “DVRs Now In Over One of Every Five U.S. Households,” Leichtman Research Group, August 21, 2007, www.leichtmanresearch.com/press/082107release.html

⁵³ Quoted in Mello, *op. cit.*

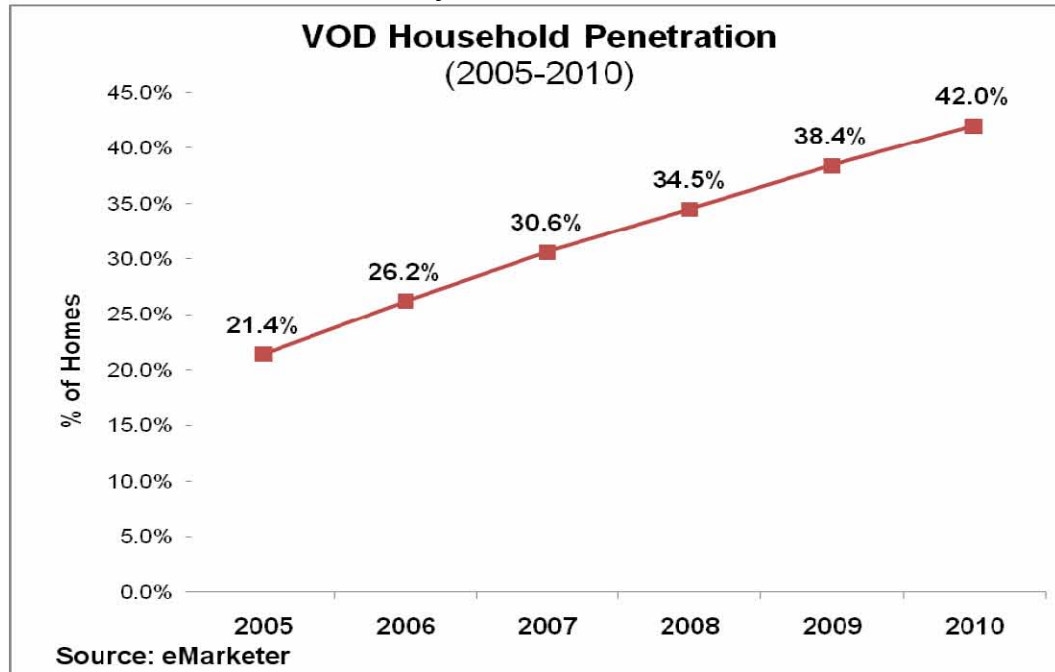
- Another market research firm, eMarketer, reports similar numbers, projecting that almost 22% of homes will have a DVR by the end of 2007.⁵⁴ eMarketer estimates that household penetration will approach 45% of all homes by 2011. (Exhibit 14 documents the projected growth of DVRs through 2011 according to eMarketer).
- DVR unit sales continue to grow at a rapid pace. The CEA reports that DVR unit sales roughly doubled between 2006 (4.9 million units) and 2007 (8.9 million), and are projected to almost double again next year (16.7 million).
- More importantly, DVR prices continue to fall steadily. The CEA reports that the average unit price for a DVR fell from \$261 in 2003 to \$177 in 2007, and it is projected to fall to \$160 by 2008. (Exhibit 15 charts the growth of unit sales versus declining unit prices for DVRs).



⁵⁴

“Growing DVR Ownership Good for TV Ads,” eMarketer, August 20, 2007, www.emarketer.com/Article.aspx?id=1005279; “30 Percent of Homes to Have DVR Capability,” eMarketer, November 28, 2006, www.emarketer.com/Article.aspx?id=1004316

Exhibit 15: Projected Growth of VOD



c) Video on demand (VOD) services

Video on demand services are also becoming more widely available to consumers, and many family-friendly options are available via VOD:

- eMarketer estimates that VOD household usage will grow from 21.4% in 2005 to 42% in 2010. (Exhibit 16 documents the projected growth of VOD).
- According to SNL Kagan, “nearly 90 percent of U.S. digital cable subscribers had access to VOD, and 46 percent of all basic cable customers were offered the service at the end of the March [2007].”⁵⁵
- Pike & Fischer estimates that each home will be watching nearly two hours of on-demand content nightly by the end of 2012.⁵⁶
- Children’s programming represents a large and quite popular portion of the overall universe of VOD programming. “The results are in: Children’s programming is a hit for video on demand,” says Matt Stump of *Multichannel News*.⁵⁷ VOD offerings from

⁵⁵ “VOD Availability Grows with Digital Platform,” *VOD & ITV Investor*, SNL Kagan, No. 106, May 30, 2007, p. 6, www.snl.com/products/samples/media_comm/kvi/sample1.pdf

⁵⁶ Scott Sleek, *Video on Demand Usage: Projections and Implications*, Pike & Fischer, October 2007, www.broadbandadvisoryservices.com/researchReportsBriefsInd.asp?repld=541

⁵⁷ Matt Stump, “Kids’ TV Rules on VOD,” *Multichannel News*, March 6, 2006, www.multichannel.com/article/CA6312983.html

Nickelodeon, the Cartoon Network, and PBS' Sprout have been wildly successful and shown that "kids' TV rules on VOD" according to Stump.⁵⁸ Last year, Comcast Corporation, the nation's largest cable provider, also found that children's programming was one of the most popular VOD categories.⁵⁹

- A Comcast poll of its most aggressive VOD and DVR users last year found that 85% of those customers indicate they "always have appropriate shows available for their children to watch." Moreover, 65% of them said that they "have fewer conflicts about what to watch on TV" and 63% said that they "watch more television as a family" thanks to these tools.⁶⁰
- A 2005 study by Marquest Research revealed approximately 29% of VOD homes with kids reported watching VOD programming three or more times per week, compared with only 12% in VOD homes without kids.⁶¹

d) *Computing devices & expanding IPTV options*

Many of these same content management tools are increasingly being bundled into PC operating systems, interactive devices, online systems, and even video game consoles.

Microsoft's Windows Media Center, for example, offers users sophisticated DVR tools to record and catalog their favorite programming.⁶² Similarly, Myth TV is a free open source program that consumers can download to give their computers DVR functionality.⁶³ Microsoft's Xbox 360 video game console also allows consumers to download television and other video programming, and Sony is planning to expand its video on demand offerings.

⁵⁸ *Id.*

⁵⁹ "Comcast On Demand Tops Three Billion Views," Comcast Corporation *Press Release*, September 6, 2006, www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=46

⁶⁰ "New National Survey Finds That On-Demand Television Services Have Positive Impact on Family Viewing Habits," Comcast Corporation, March 14, 2006, www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID=84

⁶¹ Cited in Daisy Whitney, "Kids Get Their Way on TV," *Advertising Age*, March 13, 2006.

⁶² www.microsoft.com/windowsxp/mediacenter/default.mspx and www.microsoft.com/windows/products/windowsvista/features/details/mediacenter.mspx

⁶³ www.mythtv.org

Internet protocol television, or “IPTV”, refers to a broad class of services that utilize Internet protocols to transmit digital video signals to the public.⁶⁴ Many of the new services and technologies described above, such as VOD, are built on IPTV platforms. IPTV offers the potential for much greater capacity, configurability, and interactivity than traditional television distribution and storage methods.⁶⁵

e) Falling Prices and Hyper-Tailored Content

“What’s clear is the way we watch TV has changed, and greater change is coming,” concludes *Buffalo News* reporter Stephen T. Watson.⁶⁶ Indeed, this video empowerment revolution will continue and expand. As Exhibit 17 makes clear, the prices of these video technologies will continue to fall rapidly. Very soon, almost any family that wants these technologies will find them within their reach. Already, as of September 2007, TiVo’s most popular DVR cost just \$99.99 and its latest high-definition unit recently debuted with a price tag of just \$299.99. That is stunning considering that just a few years ago, top-of-the-line DVRs had far fewer capabilities, but were selling for well over \$1,000.

⁶⁴ Nate Anderson, “An Introduction to IPTV,” *Ars Technica*, March 12, 2006, <http://arstechnica.com/guides/other/iptv.ars/1>

⁶⁵ “Essentially, IPTV has the capability of condensing down the multiple channels of conventional cable and satellite television down into one or two video-on-demand streams. What’s more, IPTV holds the promise of lots of additional content, such as statistics pop-up boxes during sporting events, extra information about the show you’re watching, integrated IM clients, and whatever other added-value widgets content providers and users can dream up.” Glenn Derene, “Buzzword: IPTV,” *Popular Mechanics*, January 17, 2007, www.popularmechanics.com/blogs/technology_news/4212160.html

⁶⁶ Stephen T. Watson, “Taking Control of the TV as DVRs Take Over,” *Buffalo News*, August 28, 2007.

Exhibit 16:
Projected Average Prices for Selected Video Technologies

	2003	2008 (est.)	% price reduction
VCRs	\$63	\$46	-27%
DVD players	\$123	\$90	-27%
DVD recorders*	\$271	\$155	-43%
DVRs	\$261	\$160	-39%
IPTV	\$175	\$119	-32%
Source: Consumer Electronics Association, <i>U.S. Consumer Sales and Forecasts, 2003-2008</i>, July 2007. *Note: First year of DVD recorder data is for 2004.			

Moreover, because many multichannel video operators essentially subsidize the cost of DVRs for their customers, it means that it will be very easy for every subscriber to have at least one in their home. “Before DVRs were a premium offering,” notes Steve Wilson, principal analyst for consumer video technologies with ABI Research. “Now they’re a standard offering.”⁶⁷

Importantly, as these technologies grow more sophisticated they will also become more user-friendly.⁶⁸ For example, TiVo already offers a feature called “TiVo Suggestions” that recommends shows users might enjoy based on their past programming choices. And TiVo’s “Universal Swivel Search” tool lets users engage in Google-like searches of their video programming lineup to find programs that match their preferences.⁶⁹ Similarly, Philips

⁶⁷ Quoted in John P. Mello, “DVR Market Penetration: Riding a Provider-Powered Wave,” *E-Commerce Times*, September 26, 2007, www.ecommercetimes.com/story/trends/59497.html

⁶⁸ “As for features, only time will tell what companies think up,” notes Andrew D. Smith of the *Dallas Morning News*. Andrew D. Smith, “Watch for More Choices from Your Cable TV Box,” *Dallas Morning News*, July 31, 2007, www.dallasnews.com/sharedcontent/dws/bus/ptech/stories/DN-cablebox_31bus.ART0.State.Edition1.35ed73d.html

⁶⁹ www.tivo.com/mytivo/domore/swivelsearch/index.html

Electronics recently demonstrated a prototype DVR that included its new “Personal TV Channel” system that quickly learns users’ preferences and creates personalized channels based on those tastes.⁷⁰ The Philips system will also be able to monitor the personal preferences of different people in the home and create specialized program lists for each of them. That would allow parents to create one preference list for themselves and another for the kids.

Such tools and features will be further refined in coming years to allow DVRs and other IPTV devices to better “learn” a user’s preferences and help them build a library of programming that is right for them and their families. At some point very soon, we might even be able to speak to these machines and communicate our preferences even more clearly. One might imagine a “conversation” with your DVR in the near future that goes something like this: “I only want my kids to see shows like *Blue’s Clues*, *Barney*, *Sesame Street*, and *Dora the Explorer*. I like shows that help develop language and musical skills such as those. But I definitely don’t want my kids to see any shows that are rated above TV-Y, or that have profanity, or that have a lot violence in them.” After hearing your commands, the DVR then retrieves a list of shows that satisfy your criteria and you refine it to ensure that it’s right for your kids.

In the future, there will also be many ways for independent organizations to “map” their content preferences onto digital empowerment devices. That is, organizations that independently rate or label media programming will be able to offer their content recommendations to media distributors so that viewers can call up shows approved by those

⁷⁰ John Blau, “Philips Readies TiVo Rival,” *IDG News Service*, September 4, 2007, www.pcworld.com/article/id,136715-page,1/article.html

groups. This is already happening today. For example, in March 2006, TiVo announced a partnership with the Parents Television Council, the Parents Choice Foundation, and Common Sense Media to jointly develop TiVo “KidZone.” Using ratings and information created by those groups, KidZone allows parents to filter and record only the content that those groups deem appropriate.⁷¹ As more content gets “tagged” by third-parties, one can image a future of infinitely searchable programming that allows parents to align their family’s viewing options with organizations they trust.

5. Family & Children’s Programming Options

The overall market for family and children’s programming options also continues to expand quite rapidly. Thirty years ago, families had a limited number of children’s television programming options at their disposal on broadcast TV. Today, by contrast, there exists a broad and growing diversity of children’s television options from which families can choose. Exhibit 18 highlights some of the more popular family- or child-oriented networks available on cable, telco, and satellite television today.

Importantly, this list does not include the growing universe of religious/spiritual television networks. Nor does it include the many family or educational programs that traditional TV broadcasters offer. Finally, the list does not include the massive market for interactive computer software or websites for children.

⁷¹ Saul Hansell, “TiVo to Offer Tighter Rein on Children’s Viewing,” *New York Times*, March 2, 2006, www.nytimes.com/2006/03/02/technology/02tivo.html?_r=1&oref=slogin

Exhibit 17: Educational / Entertainment Viewing Options for Children

- ABC Family Channel (<http://abcfamily.go.com>)
- Animal Planet (<http://animal.discovery.com>)
- Anime Network (www.theanimenetwork.com)
- Black Family Channel (www.blackfamilychannel.com)
- Boomerang (www.cartoonnetwork.com/tv_shows/boomerang)
- Cartoon Network (www.cartoonnetwork.com)
- Discovery Channel (www.discovery.com)
- Discovery Kids (<http://kids.discovery.com>)
- Disney Channel (www.disney.go.com/disneychannel)
- Encore WAM!
- Familyland Television Network (www.familyland.org/content/Content.aspx?CategoryID=51)
- FUNimation (www.funimation.com)
- Hallmark Channel (www.hallmarkchannel.com)
- Hallmark Movie Channel (www.hallmarkmoviechannel.com)
- HBO Family (www.hbofamily.com)
- History Channel (www.history.com)
- KTV – Kids & Teens Television (www.ktvzone.com)
- Learning Channel (<http://tlc.discovery.com>)
- National Geographic Channel (<http://channel.nationalgeographic.com/channel>)
- Nickelodeon (www.nick.com)
- Nick 2
- Nick Toons (<http://nicktoonsnetwork.nick.com/home.html>)
- Noggin (www.noggin.com)
- N Channel (www.the-n.com)
- PBS (www.pbs.org)
- PBS Kids (<http://pbskids.org/go>)
- Science Channel (<http://science.discovery.com>)
- Showtime Family Zone
- Sprout (www.sproutonline.com)
- Starz! Kids and Family (http://www.starz.com/appmanager/seg/s?_nfpb=true&_pageLabel=starz_kids_family)
- Toon Disney (<http://psc.disney.go.com/abcnetworks/toondisney>)
- Varsity World (www.varsityworld.com)

6. Independent Television Rating Organizations

Finally, if parents wish to independently verify official TV ratings, or just get more information about the content of specific shows, many services are available:

- Common Sense Media’s user-friendly website offers detailed TV reviews as well as user-generated reviews submitted by both parents and kids themselves.⁷² The site offers extremely detailed descriptions of almost every possible type of content that one might find in a given show.
- Plugged In Online’s website, a project of the religious group Focus on the Family, reviews many TV shows and as part of its review process considers the following elements: positive elements, spiritual content, sexual content, violent content, crude or profane language, drug and alcohol content, and other negative components.⁷³
- The Parents Television Council’s ParentsTV website offers a searchable “Family Guide to Prime Time Television”⁷⁴ and awards a seal of approval to shows that it deems suitable for families.⁷⁵
- Formed in October 2007, the Smart Television Alliance (STA) is a collection of “leading nonprofit organizations representing millions of American parents, teachers, nurses and children” that came together “to promote quality television content for children.” The STA “encourage[s] families to use information from trusted sources to identify shows that inform and educate children and to utilize technology to control what is on television and when it is watched.”⁷⁶ Founding members of the STA include the National Education Association, the National Parent Teacher Association, and the National Council of Women’s Organizations.⁷⁷ The STA bases its recommendations on the work of other groups, including: the Coalition for Quality Children’s Media: KIDS FIRST!; the Parents Television Council; the Parents’ Choice Foundation; and Common Sense Media. The STA’s website provides parents with television recommendations by age groups (ages 3-6, 6-9, and 9-11) based on the programs approved by those organizations. The STA’s website also allows families who own a TiVo personal video recorder to instantly record the shows they like directly from the website.

B. Movies

1. The MPAA Movie Rating System

The motion picture industry has the longest-running and most widely recognized rating system in America. Established by the Motion Picture Association of America (MPAA) and

⁷² www.common sense media.org/tv-reviews

⁷³ www.pluggedinonline.com/tv/index.cfm

⁷⁴ www.parentstv.org/PTC/familyguide/main.asp

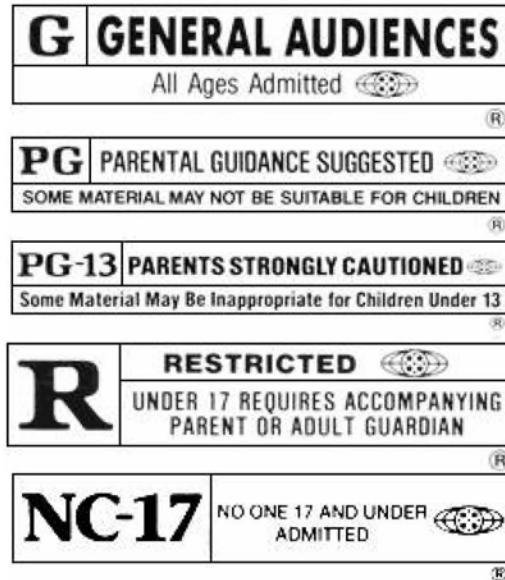
⁷⁵ www.parentstv.org/PTC/awards/main.asp

⁷⁶ “Smart Television Alliance Launched to Help Parents Access Educational Children’s TV in Response to Violent and Indecent Programming,” October 16, 2007, www.smarttelevisionalliance.org/site/PageServer?pagename=press_101607

⁷⁷ *Id.*

theater operators in 1968, the MPAA's familiar rating system includes the age-based designations are shown in adjoining exhibit.

Exhibit 18: The MPAA Movie Rating System



These ratings are accompanied by additional content descriptors explaining what viewers can expect to see in the movie. Both the ratings and content descriptors appear at the beginning of all movies—whether seen at a cinema or on VHS or DVD. When movies are sold on DVDs, the MPAA rating information is embedded on the discs in the form of machine-readable “metadata.” DVD players, gaming consoles, and other devices that can play DVDs can then read the ratings via the embedded metadata. That allows parents to block movies of a certain rating from playing on those devices.

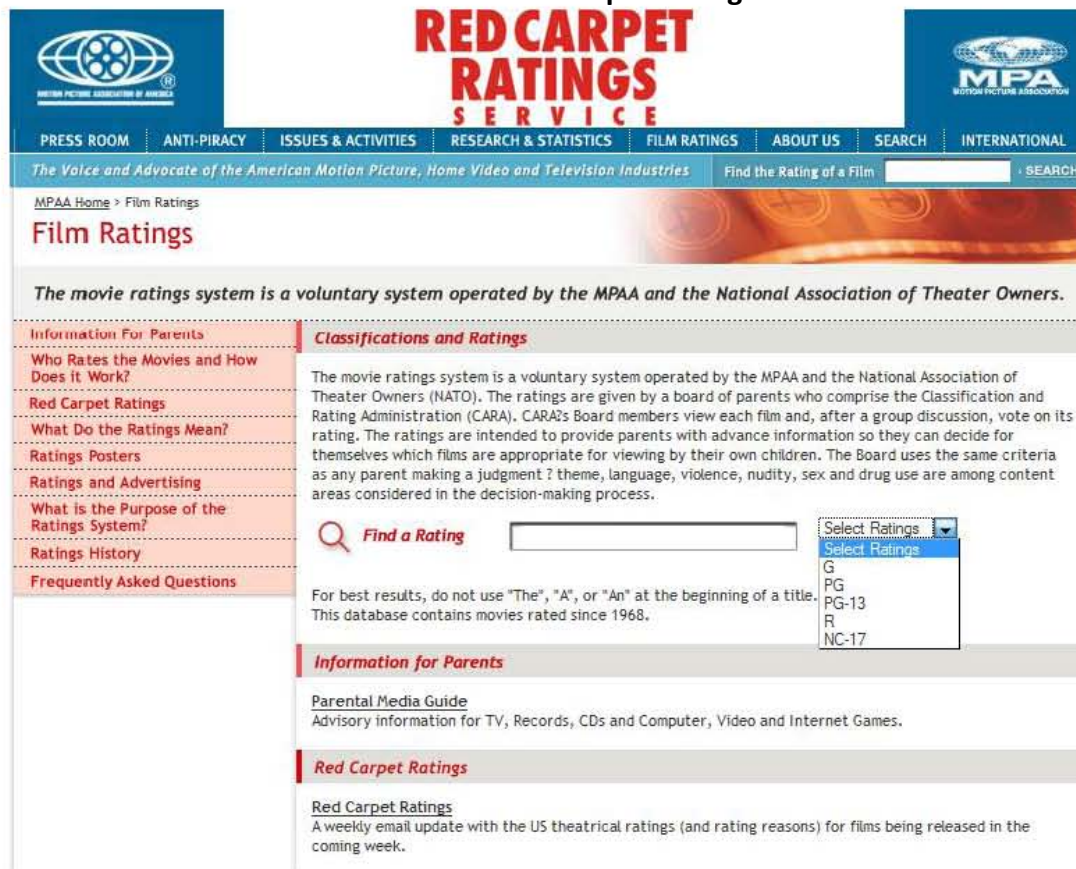
The MPAA also requires that the ratings appear on all promotional advertising (posters, TV ads, *etc.*). Finally, the MPAA's website also features a search engine that allows the public to look for any movie it has rated since 1968 and find its rating and a description of the content.⁷⁸

The MPAA also recently introduced the “Red Carpet Ratings Service,” which allows parents to

⁷⁸ www.mpa.org/FilmRatings.asp or www.filmratings.com

sign up to receive a weekly report of the ratings of recently premiered movies.⁷⁹ The MPAA has also been involved in a variety of cross-industry educational efforts.

Exhibit 19: MPAA's "Red Carpet Ratings" Service



2. Independent Movie-Rating Organizations

As was the case with TV programs, if parents wish to verify MPAA movie ratings independently, or just get more information about the content of specific movies, there are many services to which they can turn:

- Common Sense Media's user-friendly website offers detailed movie reviews as well as user-generated reviews submitted by both parents and kids themselves.⁸⁰ The site offers extremely detailed descriptions of almost every possible type of content that one

⁷⁹ www.mpa.org/FilmRat_RedCarpet.asp

⁸⁰ www.common sense media.org/movie-reviews

might find in a given title. The organization also sells a booklet summarizing *Really Great Movies for Kids & Families*.⁸¹

- The Parent Previews website reviews new theatrical releases and DVDs according to an easy-to-understand A-F grading system.⁸² Four primary categories are graded (violence, sexual content, language, and drug or alcohol use) to determine the movie's overall grade.
- Kids-in-Mind is another online rating service that assigns films three distinct, category-specific ratings: one for sex and nudity, one for violence and gore, and another for profanity. Each review provides highly detailed listings of instances of those categories within a film. Each movie's rating is on a scale of 0 to 10, depending on the quantity and context of what is shown. The site's reviews also cover other themes that parents might want to discuss with their children, such as substance abuse, divorce, or the occult.⁸³
- ScreenIt.com is an online subscription-based movie review service (\$24.95 per year) for parents looking for extremely detailed summaries of the content found in movies.⁸⁴ It evaluates each movie title using 15 different criteria.
- Plugged In Online's website, a project of the religious group Focus on the Family, reviews many movies and DVDs and as part of its review process considers the following elements: positive elements, spiritual content, sexual content, violent content, crude or profane language, drug and alcohol content, and other negative components.⁸⁵
- The Parents Television Council's ParentsTV website offers recent movie reviews⁸⁶ and awards a seal of approval to movies that it deems suitable for families.⁸⁷
- BeliefNet.com's Movie Mom website features reviews by Nell Minnow, author of *The Movie Mom's Guide to Family Movies*.⁸⁸
- The Coalition for Quality Children's Media is a national, not-for-profit organization founded in 1991 that seeks to teach children critical viewing skills and increase the visibility and availability of what it regards at quality children's programming. On its KidsFirst website, it offers critical reviews of movies and other forms of children's entertainment and provides a searchable database of recommended titles by age

⁸¹ *Really Great Movies for Kids & Families* (San Francisco, CA: Common Sense Media, 2007).

⁸² www.parentpreviews.com

⁸³ www.kids-in-mind.com

⁸⁴ www.screenit.com

⁸⁵ www.pluggedinonline.com

⁸⁶ www.parentstv.org/PTC/publications/moviereviews/main.asp

⁸⁷ www.parentstv.org/PTC/awards/main.asp

⁸⁸ <http://blog.beliefnet.com/moviemom>

group.⁸⁹ It also sponsors a film and video festival dedicated to “promoting excellence in children’s films and engaging children as film critics, curators and filmmakers.”⁹⁰

- Finally, some of the best information about what parents can expect to see and hear in movies comes from other parents who review them on sites like Amazon.com, Netflix.com, Metacritic.com, and IMDB.com (the Internet Movie Database). Indeed, most movies listed on these sites contain hundreds of user-generated reviews that typically make it very clear what the movie contains and at what approximate age it is appropriate for viewing. Unofficial sources such as The Internet Movie Database also list major ratings that each movie has received by ratings organizations worldwide.

3. Independent Movie Screening Tools

ClearPlay produces a unique DVD player that eliminates profanity, violence and nudity from certain movies.⁹¹ ClearPlay doesn’t produce pre-edited DVDs, rather, the company “create[s] filtering information on a movie by movie basis, and then put[s] those ‘filters’ into the DVD player. By doing so the DVD player knows when to skip or mute while the movie is playing.”⁹² Therefore, consumers don’t have to purchase special DVDs; they just need to purchase a ClearPlay DVD player and download the codes for their movies to activate the filtering controls. The company’s MaxPlay DVD player retails for under \$70 and comes loaded with the filters for about 1,000 popular movies. A monthly membership fee of \$7.95 is required to access new movie filtering codes.

ClearPlay’s technology raised some copyright concerns and was opposed by many movie directors and studios. But in 2005, Congress passed and President George W. Bush signed the Family Movie Act, which exempted services like ClearPlay from any copyright liability.⁹³

⁸⁹ www.kidsfirst.org/kidsfirst

⁹⁰ www.kidsfirst.org/kidsfirst/fabout.htm

⁹¹ www.clearplay.com

⁹² www.clearplay.com/about.aspx

⁹³ The Family Movie Act was part of the Family Entertainment and Copyright Act of 2005. President Bush signed the measure into law on April 27, 2005.

However, other types of preedited DVD software service—“scrubbed” DVDs—were ruled copyright violations by a U.S. district court judge in 2006 and are no longer available.⁹⁴

C. Music and Radio

1. Album Ratings

Since the mid-1980s, the music industry (working with retailers) has administered a voluntary parental advisory labeling program to give parents fair warning that a particular album might contain explicit lyrics about sex, violence, or drug use. The Recording Industry Association of America (RIAA) runs the program on behalf of record companies and producers who, working with their artists, decide which of their songs and products receive the explicit label.⁹⁵ If they determine that a warning is appropriate, the industry’s widely recognized black-and-white “Parental Advisory – Explicit Content” label is affixed prominently to the outside of the permanent packaging and embedded in the digitally delivered files. They also have an option to release a “non-explicit” version of the same song or product with the appropriate modifications.

Exhibit 20: The RIAA’s Explicit Content Parental Advisory Label



⁹⁴ Keith Regan, “Court Says Editing DVDs for Content Is Illegal,” *E-Commerce News*, July 10, 2006, www.ecommercetimes.com/story/51667.html

⁹⁵ www.riaa.com/parentaladvisory.php

Retailers also prominently display the warnings regardless of how they choose to offer music products for sale—retail or digital. Many retailers have long-established procurement guidelines and refuse to sell “Explicit” labeled products to those younger than 18. Other retailers, such as Wal-Mart, refuse to carry such albums at all.

2. Satellite Radio Controls

SIRIUS-XM, a satellite radio service, offers subscribers a variety of plans to choose from including several that exclude any channels that might include programming with explicit language or lyrics. For example, the “Family Friendly” package⁹⁶ excludes 17 channels⁹⁷ that feature explicit language or graphic content. Alternatively, subscribers can simply purchase channels on an *a la carte* basis and avoid the channels they might find objectionable.⁹⁸ Subscribers can also request that certain channels be blocked by contacting the SIRIUS customer service department.⁹⁹

3. Apple iPod and Microsoft Zune Parental Controls

Not every portable music player on the market today offers embedded parental control capabilities, but two major competitors in this space—Apple and Microsoft—do offer some controls on their devices and have standing commitments to improve these capabilities over time by working together with the music industry in standards-settings organizations.

Apple’s wildly successful iPod is by far the most popular portable music player on the market today. Once users purchase an iPod, they also download iTunes software onto

⁹⁶ www.sirius.com/packages/more#family

⁹⁷ www.sirius.com/mature

⁹⁸ www.sirius.com/packages/more#alacarte

⁹⁹ www.sirius.com/dodge/faq.html#q8

computers to transfer music onto their player or buy material online at Apple's iTunes Store.¹⁰⁰

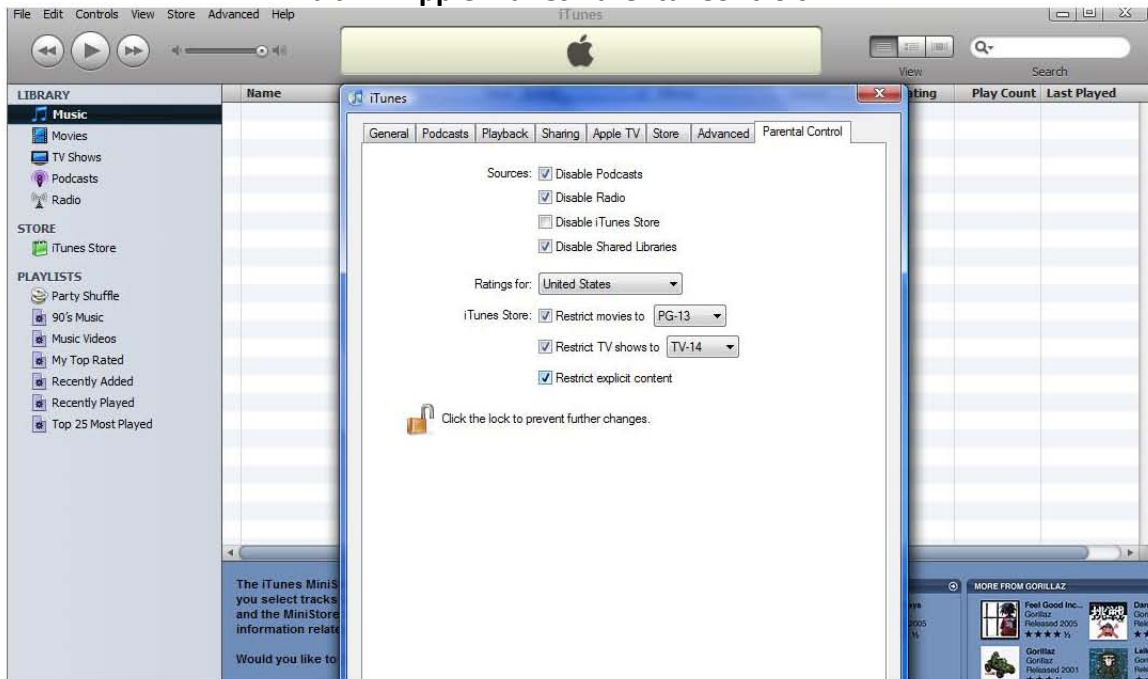
At the iTunes Store, users can purchase songs and videos or download free online radio stations or podcasts. Music singles containing explicit lyrics have a bold red "EXPLICIT" label next to song title. Movies are clearly labeled with MPAA movie ratings and other content descriptors making it clear what type of content can be found in the title.

Parents can find parental controls in the iTunes software on the main menu under "Edit / Preferences / Parental Controls." Once there, they can disable all podcasts, online radio and music sharing, or they can disable access to the iTunes Store altogether. Less drastically, if they want to make the iTunes Store accessible, but limit what can be downloaded, they can designate the level of movie and TV ratings that are appropriate for their children and nothing rated above that level will be accessible. Furthermore, parents can restrict the downloading of any music that contains the "EXPLICIT" label on the site. Once appropriate settings are determined, parents can lock the software to prevent further changes.

¹⁰⁰

www.apple.com/itunes/store

Exhibit 21: Apple iTunes Parental Controls



Microsoft's Zune portable media player also offers family settings that allow parents to control what their children can download from the Zune Marketplace website. Before a child can create an online Zune account he or she must have parental consent:

When your child first signs up online for Zune, they enter (or you enter for them) their own Windows Live ID and account information, and then Zune asks for parental permission to continue creating the account. You give parental permission by using or creating a master Windows Live ID and entering some credit card information to verify that you are an adult. (The credit card is not charged.)¹⁰¹

Parents can also establish their own family settings when creating an account for their children. Specifically, parents determine whether to allow their kids to purchase premium content or explicit content on the Zune Marketplace website. Like the iTunes Store, Microsoft's Zune Marketplace contains some material marked as "explicit" and allows parents to block such

101

www.zune.net/en-us/support/howto/marketplace/familysettings.htm

material from being downloaded by their children. Parents can alter the settings at any time by going to the main menu and clicking “Account Management / Family Settings.”

Importantly, new music industry product identification solutions are developing that will facilitate parental control technologies in the future. For example, the Global Release Identifier (GRID) is the recording industry’s new product identification system that encourages those in the industry to embed product metadata in their digital music files.¹⁰² And the Digital Data Exchange (DDEX) is the music industry’s system for reporting and tracking these new digital music IDs.¹⁰³

GRID and DDEX are primarily used by music companies, device manufacturers, service providers, and technology implementers to track sales, gauge royalties, and monitor piracy. But embedded metadata can also include digital content labels and rating information that can facilitate screening capabilities. For example, on its Zune webpage, Microsoft outlines the type of metadata labels that content creators can include in their digital files that can then be read by the Zune.¹⁰⁴ Parental ratings—for music, movies, and television—are among the metadata labels that Microsoft recommends. As these metadata labeling efforts expand, other consumer electronic device makers will also be able to include parental controls in their products that can read media labels and ratings. This will make it easier for parents to restrict potentially objectionable or age-inappropriate content on music players or other mobile media devices.

¹⁰² www.ifpi.org/content/section_resources/grid.html

¹⁰³ www.ddex.net/index.htm

¹⁰⁴ www.zune.net/en-us/support/howto/start/providecontent.htm#section7

4. Independent Rating Organizations

Once again, as is the case with TV, movies, and video games, parents who want more information about the music their kids might want can use independent websites for their research. Common Sense Media.org provides detailed music reviews and details what parents can expect their kids to hear in the music they buy. Similarly, Plugged In Online¹⁰⁵ focuses on the “pro-social content” versus “objectionable content” found on each album it reviews. And user-generated reviews on sites like Amazon.com¹⁰⁶ and Metacritic.com¹⁰⁷ feature excellent product summaries that can help parents decide if various music titles are right for their kids. Finally, if parents want to examine the lyrics of the songs their children are listening to, they can find them at sites such as A-Z Lyrics Universe,¹⁰⁸ Lyrics.com¹⁰⁹ and LyricsMania.com.¹¹⁰

D. Video Games

1. The ESRB Rating System

Although it is the newest of all industry content rating and labeling schemes, the video game industry’s system is in many ways the most sophisticated, descriptive, and effective ratings system ever devised by any major media sector in America. Established by the video game industry in 1994, the Entertainment Software Rating Board (ESRB) is a self-regulatory rating and labeling body.

¹⁰⁵ www.pluggedinonline.com/music

¹⁰⁶ www.amazon.com

¹⁰⁷ www.metacritic.com

¹⁰⁸ www.azlyrics.com

¹⁰⁹ www.lyrics.com

¹¹⁰ www.lyricsmania.com

Exhibit 22: ESRB Video Game Ratings System¹¹¹

ESRB Rating Symbols

	<p>EARLY CHILDHOOD</p> <p>Titles rated EC (Early Childhood) have content that may be suitable for ages 3 and older. Contains no material that parents would find inappropriate.</p>
	<p>EVERYONE</p> <p>Titles rated E (Everyone) have content that may be suitable for ages 6 and older. Titles in this category may contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language.</p>
	<p>EVERYONE 10+</p> <p>Titles rated E10+ (Everyone 10 and older) have content that may be suitable for ages 10 and older. Titles in this category may contain more cartoon, fantasy or mild violence, mild language and/or minimal suggestive themes.</p>
	<p>TEEN</p> <p>Titles rated T (Teen) have content that may be suitable for ages 13 and older. Titles in this category may contain violence, suggestive themes, crude humor, minimal blood, simulated gambling, and/or infrequent use of strong language.</p>
	<p>MATURE</p> <p>Titles rated M (Mature) have content that may be suitable for persons ages 17 and older. Titles in this category may contain intense violence, blood and gore, sexual content and/or strong language.</p>
	<p>ADULTS ONLY</p> <p>Titles rated AO (Adults Only) have content that should only be played by persons 18 years and older. Titles in this category may include prolonged scenes of intense violence and/or graphic sexual content and nudity.</p>
	<p>RATING PENDING</p> <p>Titles listed as RP (Rating Pending) have been submitted to the ESRB and are awaiting final rating. (This symbol appears only in advertising prior to a game's release.)</p>

The ESRB rating scheme is remarkably comprehensive. According to the ESRB, it rates well over 1,000 games per year in most years and it rated 1,563 games in 2007. Virtually every title produced by major game developers for retail sale today carries an ESRB rating and

¹¹¹ www.esrb.org/ratings/ratings_guide.jsp

content descriptors. Generally speaking, the only games without ESRB ratings today are those developed by web amateurs that are freely traded or downloaded via the Internet. The ESRB applies seven different rating symbols to the games it rates. The adjoining exhibit describes these ratings.

In addition to designating these ratings, the ESRB has over 30 different content “descriptors” that it uses to give consumers highly detailed information about games. Thus, by simply glancing at the back of each game container, parents can quickly gauge the appropriateness of the title for their children. If parents want to do additional research in advance of a purchase, the ESRB’s website allows them to enter the name of any game and retrieve its rating and various content descriptors. Moreover, in March 2008, the ESRB began offering an “ESRB Rating Search Widget” that can be freely downloaded and installed on a user’s computer.¹¹² It allows users to instantly search for any game title and retrieve its rating and content descriptors. Also, in November 2008, the ESRB announced it would be offering game “rating summaries” that offered “supplementary source of information about game content that parents can use when considering which games to purchase for their children.”¹¹³ Those rating summaries will be accessible when searching for rating information via the ESRB website or through the ESRB search widget.

¹¹² www.esrb.org/about/widget/widget-consumer.jsp

¹¹³ “ESRB Announces New Video Game Rating Summaries,” ESRB *Press Release*, November 12, 2008, www.esrb.org/about/news/downloads/ESRB_Rating_Summaries_Release_11.12.08.pdf

Exhibit 23: ESRB Content Descriptors

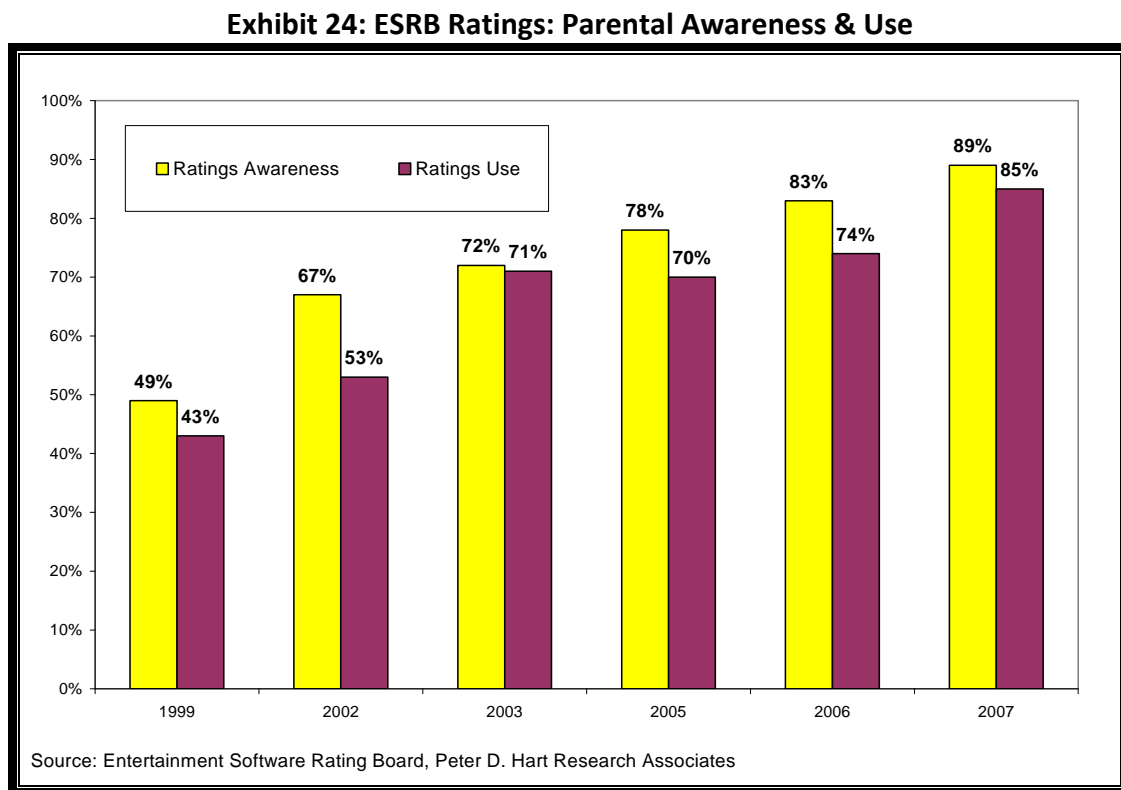
- **Alcohol Reference** - Reference to and/or images of alcoholic beverages
- **Animated Blood** - Discolored and/or unrealistic depictions of blood
- **Blood** - Depictions of blood
- **Blood and Gore** - Depictions of blood or the mutilation of body parts
- **Cartoon Violence** - Violent actions involving cartoon-like situations and characters. May include violence where a character is unharmed after the action has been inflicted
- **Comic Mischief** - Depictions or dialogue involving slapstick or suggestive humor
- **Crude Humor** - Depictions or dialogue involving vulgar antics, including "bathroom" humor
- **Drug Reference** - Reference to and/or images of illegal drugs
- **Fantasy Violence** - Violent actions of a fantasy nature, involving human or non-human characters in situations easily distinguishable from real life
- **Intense Violence** - Graphic and realistic-looking depictions of physical conflict. May involve extreme and/or realistic blood, gore, weapons and depictions of human injury and death
- **Language** - Mild to moderate use of profanity
- **Lyrics** - Mild references to profanity, sexuality, violence, alcohol or drug use in music
- **Mature Humor** - Depictions or dialogue involving "adult" humor, including sexual references
- **Nudity** - Graphic or prolonged depictions of nudity
- **Partial Nudity** - Brief and/or mild depictions of nudity
- **Real Gambling** - Player can gamble, including betting or wagering real cash or currency
- **Sexual Content** - Non-explicit depictions of sexual behavior, possibly including partial nudity
- **Sexual Themes** - References to sex or sexuality
- **Sexual Violence** - Depictions of rape or other violent sexual acts
- **Simulated Gambling** - Player can gamble without betting or wagering real cash or currency
- **Strong Language** - Explicit and/or frequent use of profanity
- **Strong Lyrics** - Explicit and/or frequent references to profanity, sex, violence, alcohol or drug use in music
- **Strong Sexual Content** - Explicit and/or frequent depictions of sexual behavior, possibly including nudity
- **Suggestive Themes** - Mild provocative references or materials
- **Tobacco Reference** - Reference to and/or images of tobacco products
- **Use of Drugs** - The consumption or use of illegal drugs
- **Use of Alcohol** - The consumption of alcoholic beverages
- **Use of Tobacco** - The consumption of tobacco products
- **Violence** - Scenes involving aggressive conflict. May contain bloodless dismemberment
- **Violent References** - References to violent acts

To ensure that its system is enforced properly under all cross-platform scenarios, the console manufacturers require that the rating is digitally available in the metadata or product description so the console or PC can identify and screen the content in advance.

Surveys have shown that most parents find the ratings and labels very helpful. Studies by Peter D. Hart Research Associates reveal that:¹¹⁴

- 89% of American parents of children who play video games are aware of the ESRB ratings;
- 85% consult the ratings regularly when buying games for their families; and
- 90% say the ratings are very to somewhat helpful in buying or renting games for their kids.

As the adjoining exhibit illustrates, these results have been increasing steadily since Hart Research Associates began conducting these surveys for the ESRB in 1999.

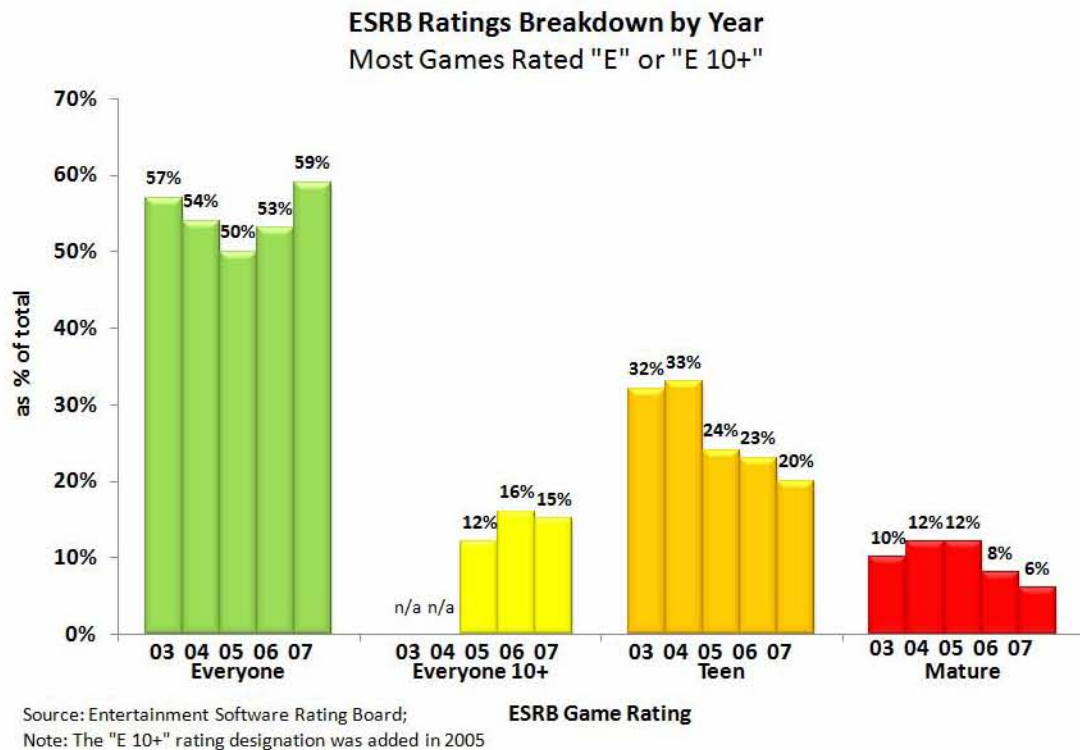


Importantly, surveys conducted by the Entertainment Software Association (ESA), which represents the video game industry, have also shown a high level of parental involvement when

¹¹⁴ "Parents Increasingly Using ESRB Ratings to Restrict the Video Games Their Children Play," Entertainment Software Rating Board *Press Release*, May 4, 2007, www.esrb.org/about/news/downloads/ESRB_AwarenessUsePR_5.4.07.pdf

games are purchased or rented. According to ESA surveys, the average age of a video game purchaser is 40, and 94% of the time parents are present when games are purchased or rented.¹¹⁵ Of parents surveyed, 88% said they always or sometimes monitoring the games their children play.¹¹⁶

Exhibit 25: Video Game Ratings By Year



Incidentally, contrary to popular belief, the vast majority of video games the ESRB rates are not filled with violent content. As the Exhibit 27 reveals, well over 50% of ratings assigned by ESRB are for titles rated "E" for "Everyone," and adding in those titles rated "E10+" boosts the annual total over 60% most years, and 70% more recently. Meanwhile, the number of

¹¹⁵ *Essential Facts about the Computer and Video Game Industry: 2008 Sales, Demographics and Usage Data*, Entertainment Software Association, 2008, p. 3, 6, www.theesa.com/facts/pdfs/ESA_EF_2008.pdf

¹¹⁶ *Id.*, p. 7.

games rated “T” for “Teen” or “M” for “Mature” has been falling relative to the other options available. Consequently, it would be difficult for policymakers or game critics to build the case for video game regulation on the contention that most games made today contain extreme violence or sexuality. Moreover, while it is true that games rated “T” can include some violent content, it is typically not the sort of violence that would rise to a level of serious concern for most parents. For example, lightsaber fights in “Star Wars” games or knockouts in boxing games might qualify those titles for “T” ratings, but is that really the sort of violence that concerns most parents? It’s unlikely.

The ESRB also operates an Advertising Review Council (ARC) that promotes and monitors advertising and marketing practices in the gaming industry. The ARC monitors compliance with ESRB guidelines and places restrictions on how game developers may market ESRB-rated games through its “Principles for Responsible Advertising” and “Advertising Code of Conduct.”

As part of its “OK to Play?” education campaign, the ESRB provides a variety of materials to retailers. The materials include an ESRB employee training manual and quiz about the rating system. According to the ESRB, the “OK to Play?” signage is displayed at 17 top national retailers who account for approximately 90% of all game sales. Prominent retailers involved in the effort include Wal-Mart, Best Buy, Target, Toys-R-Us, and EB Games among others. These retailers, which are responsible for a significant portion of all video game sales, have enormous reputational incentives to abide by the ESRB rating system. Importantly, the in-store signage used by these and other game retailers is also reproduced as consumer advertising in various magazines, newspapers, websites, etc.

Finally, in November 2006 the ESRB announced an educational partnership with the Parent-Teacher Association (PTA) to “encourage and enable state and local PTAs to educate their community’s parents about the [ESRB] ratings.”¹¹⁷ As part of this new education campaign, 1.3 million brochures will be distributed to 26,000 PTAs nationwide in both English and Spanish. Additional online support and downloadable manuals and educational material are available on both the ESRB and PTA websites.¹¹⁸ The ESRB has also cosponsored several TV PSAs that were supported by legislators such as Senators Hillary Clinton and Joe Lieberman,¹¹⁹ and state attorneys general Mark Shurtleff of Utah and Thurbert Baker of Georgia. In these TV spots, public officials encourage parents to use the video game ratings when buying games for their children.¹²⁰

The ESRB’s education and awareness-building efforts appear to be paying off, including at the point of sale regarding underage efforts to buy games. Since 2000, the Federal Trade Commission (FTC) has surveyed the marketing and advertising practices of major media sectors (movies, music and video games) in an annual report entitled *Marketing Violent Entertainment to Children*.¹²¹ The agency hires a research firm that conducts “secret shopper” surveys to see how well voluntary media rating systems (MPAA, ESRB, RIAA) are being enforced at the point of

¹¹⁷ “PTA and ESRB Launch Nationwide Video Game Ratings Educational Partnership,” Parent Teacher Association *Press Release*, November 15, 2006, www.pta.org/ne_press_release_detail_1163547309281.html

¹¹⁸ www.esrb.org/about/pta_partnership.jsp

¹¹⁹ “Senators Hillary Rodham Clinton and Joe Lieberman Join ESRB to Launch Nationwide Video Game Ratings TV PSA Campaign,” Entertainment Software Rating Board *Press Release*, December 7, 2006, www.esrb.org/about/news/12072006.jsp

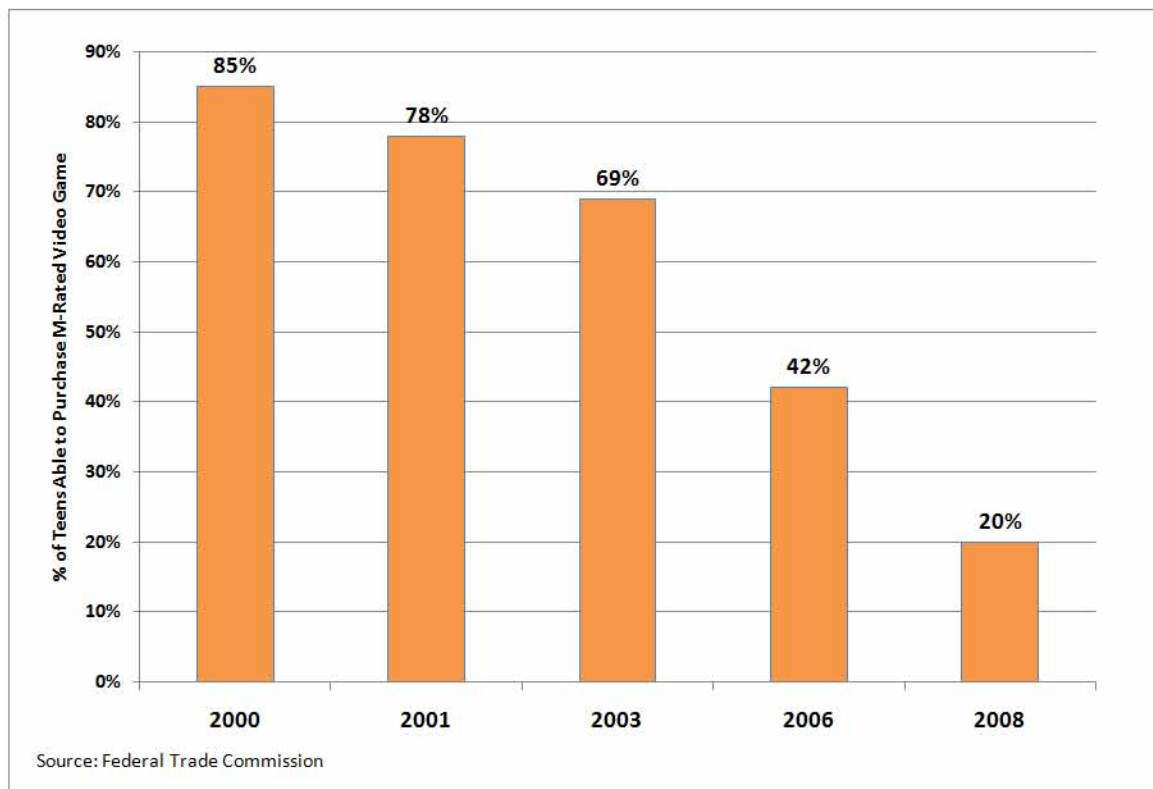
¹²⁰ These videos can be viewed at the “Media Library” on the ESRB website: www.esrb.org/about/media_library.jsp

¹²¹ Past FTC reports can be found at: www.ftc.gov/bcp/online/edcams/ratings/reports.htm

sale. The research firm then recruits a number of 13- to 16-year-olds who make an attempt to purchase such media without a parent being present.

The FTC reports show that ratings enforcement has generally been improving over time, and in the case of the ESRB system, it has improved dramatically. For example, the latest survey shows that, whereas 85% of kids were able to purchase a M-rated video games in 2000, only 20% of them were able to do so when the most recent survey was conducted in 2008.¹²² That is an impressive turn-around in a very short period of time.

Exhibit 26: FTC “Secret Shopper” Surveys Show Improved Retailer Enforcement



¹²²

“Undercover Shoppers Find it Increasingly Difficult for Children to Buy M-Rated Games,” Federal Trade Commission, *Press Release*, May 8, 2008, www.ftc.gov/opa/2008/05/secretshop.shtm

2. Video Game Console Blocking Controls

Parents have another line of defense once video games are brought into their homes. Major game console developers (Microsoft,¹²³ Sony,¹²⁴ and Nintendo¹²⁵) all recognize ESRB's digitally embedded ratings and offer blocking tools in their new gaming systems.¹²⁶ For example, the Microsoft Xbox 360 and the Nintendo Wii consoles allow parents to enter the ESRB rating level that they believe is acceptable for their children. Once they do so, no game rated above that level can be played on the console.

All ESRB-rated games contain embedded metadata "flags," or a string of code in the software, that allow the consoles to automatically recognize the game's rating. (Personal computers using the new Microsoft Windows Vista operating platform have the same screening capabilities as these stand-alone gaming consoles.)¹²⁷

Thus, parents could set the rating threshold on their child's video game console or personal computer to T for Teen and then no games rated Mature (M) or Adults Only (AO) could be played on the console unless the parent first enters a password. (These controls can also be used to block movie playback according to the MPAA ratings.)

¹²³ www.xbox.com/en-US/support/familysettings/xbox360/familysettings-intro.htm

¹²⁴ Instructions for how to do so on the PlayStation3 can be found under the "Parental Controls" tab at: www.us.playstation.com/SCEARegionalOnlineManual/frame_hardware.html

¹²⁵ www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

¹²⁶ See generally Mike Musgrove, "A Computer Game's Quiet Little Extra: Parental Control Software," *Washington Post*, December 23, 2006, p. D1, www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122201278.html

¹²⁷ This system works cross-platform because the game industry has reached a consensus on how to embed ratings information in a standard way. Film, music, and television industries are considering similar methods for their commercial products.

Exhibit 27: Microsoft Xbox Parental Control Set-Up Menus



Sony's PlayStation 3 console and PlayStation Portable (PSP) handheld gaming system work a little differently. Both Sony gaming products let parents use a 1-11 scale to determine the level of game and DVD content they will allow their kids to play. (Roughly speaking, "2" on the Sony scale = "EC" while "10" = "AO").

In November 2007, Microsoft announced that it was also offering Xbox 360 owners the ability to employ a new “Family Timer” feature.¹²⁸ Using the Family Timer, parents can limit how and when children play games on the console. This is similar to the time management tools Microsoft offers in its new Vista operating system for PCs (discussed below). The Family Timer upgrade was made available to consumers via a downloadable update feature available on any console connected to the Internet. When announcing the Family Timer, Microsoft also launched a new awareness campaign in conjunction with the Parent Teacher Association (PTA) referred to as the “Is Your Family Set?” campaign.¹²⁹ At the same time, Microsoft and the PTA also rolled out a new “P.A.C.T.” agreement form that parents and their children could sign to reach an agreement on acceptable video game usage in the home.¹³⁰ And in early 2009, Microsoft launched a new portal, GetGameSmart.com, which aggregates all these tools and efforts.¹³¹

The ESA survey cited above has found that 75% of parents surveyed found these video game console parental control tools to be useful.¹³²

3. Online, Multiplayer Gaming

Online gaming and what are referred to as “massively multiplayer online games” (“MMOGs”) are the hottest thing in the gaming world today. A user must have an Internet

¹²⁸ “Microsoft, PTA and Super Bowl Champion Jerry Rice Announce New Tools to Help Parents Manage Kids’ Interactive Media Use,” Microsoft *Press Release*, November 7, 2007, www.microsoft.com/presspass/press/2007/nov07/11-07FamilyTimerPR.mspx

¹²⁹ www.xbox.com/en-US/support/familysettings

¹³⁰ “P.A.C.T.” stands for “Parental involvement, Access, Content and Time. See http://assets.xbox.com/en-US/support/familysettings/MS_Pact_021308a.pdf

¹³¹ www.getgamesmart.com

¹³² *Essential Facts about the Computer and Video Game Industry: 2008 Sales, Demographics and Usage Data*, Entertainment Software Association, 2008, p. 8, www.theesa.com/facts/pdfs/ESA_EF_2008.pdf

connection—usually a high-speed broadband connection—to interact in these online environments. Once they are connected, players can interact with countless other gamers, some of whom will be friends, but many will be strangers.

That fact will obviously raise some concern for some parents. While the ESRB can rate game content for traditional, individual game play, it cannot rate or perfectly describe how the gaming experience might change while online since game play is spontaneously shaped by multiple participants. This is why many online games sold today include an additional warning to parents that reads, “Game Experience May Change During Online Play.” This makes it clear that user-generated content or online social interaction cannot be rated by the ESRB.

Parents have a couple of options at their disposal. First, they can disable online gaming capabilities altogether by either (a) not connecting the gaming console to an Internet connection or (b) using the controls embedded in new gaming consoles to disable or limit online connections. This approach is particularly sensible if parents allow their children to start gaming at a young age.

Exhibit 28: Microsoft Xbox Communications Blocking Controls



Second, parents can allow limited online gaming, but demand that their children play with only known, trusted acquaintances. This process can be automated in the new Microsoft Xbox 360,¹³³ Sony PS3,¹³⁴ and Nintendo Wii¹³⁵ gaming consoles by restricting access to the child's friends list or gamer profile. In other words, parents can build the equivalent of a "buddies list" for their kids and allow them to play with only those other children. Alternatively, the systems enable parents to allow online gaming, but restrict the chat capabilities so others cannot talk to their children. Incidentally, parents can also view a list of whom their children have been playing by examining the list of other gamers with whom they have interacted during online sessions. And parents can also limit how much children can spend in online "marketplaces" and set the limit to zero if they do not want their kids buying any online content. Integrated Internet browser capabilities can be turned off entirely.

Third, as their children get older and are allowed more interactive gaming, parents should ask them to report any suspicious communications from strangers in these games. Parents can report such behavior to online gaming operators who will take appropriate steps if undesirable activities are detected.

4. Independent Video Game Rating Organizations

As was the case with TV, movie, and music ratings, if parents wish to verify ESRB game ratings independently, or just want more information about what their kids might see or hear in the games they buy them, several services are at their disposal. Websites such as Common

¹³³ Instructions for how to do so on the Xbox 360 can be found at: www.xbox.com/en-US/support/familysettings/console/xbox360/consolefamilysettings.htm

¹³⁴ Instructions for how to do so on the PlayStation3 can be found under "Creating an Account" and "Going Through the Registration Process" at: www.us.playstation.com/content/sites/176/info/frame_network.html

¹³⁵ www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

Sense Media,¹³⁶ What They Play,¹³⁷ Gamer Dad,¹³⁸ Game Pro Family¹³⁹ and Children's Technology Review¹⁴⁰ provide detailed video game reviews and information about the specific types of content that kids will see or hear in a game.¹⁴¹ And user-generated reviews on sites like Amazon.com¹⁴² and Metacritic.com¹⁴³ feature excellent product summaries, often written by other parents, which can help parents decide if games are right for their kids.

E. Wireless & Mobile Media

Cell phones and other handheld mobile media devices have taken the world by storm. According to CTIA, the wireless industry's trade association, there were over 260 million estimated cellular telephone subscribers in America as of summer 2008.¹⁴⁴ That is an astonishing number considering that few of us carried mobile devices in our pockets just 10 years ago. Today, however, even young children have their own cell phones.

Importantly, cell phones are becoming much more than just communication devices; they are now full-fledged multimedia platforms capable of delivering video, data, games,

¹³⁶ www.common sense media.org/game-reviews. In May 2007, electronic retailing giant Best Buy announced that, in addition to ESRB ratings, it would begin using Common Sense Media's ratings in its stores and online to provide parents with more information about the games their kids desire. See Carissa Wyant, "Best Buy Launches Video Game Rating System for Parents," *Minneapolis / St. Paul Business Journal*, May 16, 2007, <http://twincities.bizjournals.com/twincities/stories/2007/05/14/daily19.html>

¹³⁷ www.whattheyplay.com

¹³⁸ www.gamerdad.com

¹³⁹ www.gameprofamily.com

¹⁴⁰ www.childrenssoftware.com

¹⁴¹ The ESRB keeps a running list of resources for parents at: www.esrb.org/about/resources.jsp

¹⁴² www.amazon.com

¹⁴³ www.metacritic.com

¹⁴⁴ www.ctia.org

instant messages, and more.¹⁴⁵ Subscribers can use these devices to access news, information and entertainment from almost anywhere.

Of course, this otherwise wonderful development has some downsides for parents who are concerned about the types of inappropriate content their children might be able to access on mobile devices.¹⁴⁶ And, according to the Yankee Group, 72% of teens between ages 13 and 17 already have a mobile phone, and that number continues to grow.¹⁴⁷ Consequently, kids need to be taught proper mobile phone etiquette,¹⁴⁸ and parents also need to consider strategies and tools that can help guide appropriate use. “Luckily for parents, new software is allowing parental control like never before,” notes Lee Ferran of *ABC News*.¹⁴⁹

1. Wireless Carrier Guidelines

For example, the wireless industry is responding to this concern in a preemptive fashion. In November 2005, CTIA unveiled new “Wireless Content Guidelines” that industry members would follow “to proactively provide tools and controls to manage wireless content offered by

¹⁴⁵ “[T]he devices we call ‘mobile phones’ are, in fact, PCs. They’re just another computer form factor. Some PCs are desktops. Some are laptops. And some are handhelds.” Sascha Segan, “Think of Cell Phones Like Miniature PCs,” *PC Magazine*, June 26, 2007, p. 80, www.pcmag.com/article2/0,1895,2139510,00.asp.

¹⁴⁶ As *Wall Street Journal* reporter Dionne Searcey notes, “Parents have been clamoring for more controls, especially as phones have morphed into minicomputers... [with] capabilities that make some parents nervous.” Dionne Searcey, “Keeping Junior on a Wireless Leash,” *Wall Street Journal*, September 4, 2007, p. D1.

¹⁴⁷ Joseph De Avila, “Quelling the Danger Lurking In Junior’s Backpack,” *Wall Street Journal*, April, 23, 2008, p. D1, http://online.wsj.com/public/article/SB120891052219636621-XIICJVxolbk9xAXrUAzV7IZXnb8_20080522.html?mod=tff_main_tff_top

¹⁴⁸ The Harvard University Center on Media and Child Health has some useful guidelines here: <http://cmch.tv/mentors/hotTopic.asp?id=70>. Also, the National Institute on Media and the Family produces an excellent guide for parents entitled “Cell Phones and Your Kids” that offers friendly pointers for parents looking to teach their children proper cell phone etiquette. See *A MediaWise Parent Guide—Cell Phones and Your Kids*, (Minneapolis, MN: National Institute on Media and the Family, 2006), www.mediafamily.org/network_pdf/cellphon_guide.pdf

¹⁴⁹ Lee Ferran, “Parental Controls for Cell Phones,” *ABC News.com*, December 26, 2008, www.abcnews.go.com/GMA/Parenting/story?id=6529871&page=1

the carriers or available via Internet-enabled wireless devices.”¹⁵⁰ Under the guidelines, wireless carriers pledged not to offer any adult-oriented content until they have created controls to allow parents to restrict access.¹⁵¹

The guidelines propose the creation of a Content Classification Standard, which will divide mobile content into two categories: (a) “Generally Accessible Carrier Content” and (b) “Restricted Carrier Content.” Ratings will then be developed using familiar categories and criteria employed by existing movie, television, music and games rating systems; and then tools will be developed to “ensure carrier-offered content either excludes or requires parent or guardian permission to access any material inappropriate for subscribers under 18.”¹⁵² Under the second phase of the plan, wireless carriers will implement Internet Content Access Control technologies to let consumers block access to the Internet entirely or block access to specific websites that they might find inappropriate.¹⁵³




¹⁵⁰ “Wireless Carriers Announce ‘Wireless Content Guidelines,’” *CTIA Press Release*, November 8, 2005, <http://www.ctia.org/media/press/body.cfm/prid/1565>

¹⁵¹ See Amol Sharma, “Wireless Carriers Set Strict Decency Standards for Content,” *Wall Street Journal*, April 27, 2006, p. B1.

¹⁵² *Id.*

¹⁵³ The complete guidelines can be found at www.ctia.org/consumer_info/service/index.cfm/AID/10394 and the classification criteria for “Restricted Carrier Content” can be found at www.ctia.org/content/index.cfm/AID/10395

Exhibit 29: Verizon Wireless Content Rating System

Verizon Wireless Content Ratings	
 <p>Ages 7+</p>	<p>This material contains little or no violence, no strong language, little or no sexual dialogue and situations and no themes of a mature nature. This content is considered suitable for children age 7 and above and parents can comfortably allow this content to be accessed by children 7 and above unattended.</p>
 <p>Ages 13+</p>	<p>This material may contain mild coarse language, moderate violence, some sexuality or suggestive dialogue or themes that may not be appropriate for younger children. This content would be considered suitable for children 13 and above by most parents. Parents are cautioned against allowing children under 13 to access or view this content unattended.</p>
 <p>Ages 17+</p>	<p>This content may contain one or more of the following: strong language, violence, nudity, sexual situations, or drug abuse. Many parents would consider this material unsuitable for children under 17 and parents are strongly cautioned against allowing children under 17 to access or view this content.</p>
<p>FILTER OFF</p>	<p>Turning off the content filter provides access to all content accessible through your mobile phone, including content that you may consider objectionable due to the ages of your children or your personal desire to avoid certain types of content.</p> <p>Please note: Some content may require additional authentication and/or age verification prior to access, download, use or purchase.</p>

Beyond restricting access to inappropriate content, these carriers help parents set customize limits for each child according to age. Although details vary by provider, parents can also generally manage how and when kids use their phones, including limitations on the overall minutes used for messaging and downloads. The plans can even restrict who the child can contact with their phones.¹⁵⁴ For example, using AT&T's new "Smart Limits for Wireless," AT&T customers can determine specifically how and when their kids use their phones. Parents can limit the number of text and instant messages; the dollar amount of downloadable purchases (e.g., ringtones, games); when the phone can be used for calling or texting; and access to inappropriate content.¹⁵⁵ Many carriers now also offer global positioning system (GPS) tracking

¹⁵⁴ Dionne Searcey, "Keeping Junior on a Wireless Leash," *Wall Street Journal*, September 4, 2007, p. D1.

¹⁵⁵ www.wireless.att.com/learn/articles-resources/parental-controls/smart-limits.jsp

technology in their phones, which allows parents to locate their children and monitor their whereabouts.¹⁵⁶

Independent services are also being developed that supplement these industry efforts. For example, Radar, which bills itself as “Your Kids’ Mobile Watchdog,” is a new service that “monitors and tracks your child's cell phone contacts and immediately alerts you if he or she receives unwanted or suspicious email, Instant Messages, text messages or phone calls.”¹⁵⁷ If the child is contacted by an unapproved person, parents are immediately sent an alert on their phones and via e-mail. And parents are alerted when children add new friends to their device.¹⁵⁸ The Radar service costs \$10/month for one user or \$15/month for an entire family.

CTIA has also developed an awareness campaign called “Get Wise about Wireless,” which “helps educate students about cell phone use and the responsible behaviors associated with using cell phones.”¹⁵⁹ The program includes a variety of materials such as a teacher’s guide and a family take-home pamphlet about safe and courteous cell phone use.¹⁶⁰ As part of this effort, CTIA also runs a student essay contest about sensible wireless use.¹⁶¹

¹⁵⁶ Larry Magid, “Global Positioning by Cellphone,” *New York Times*, July 19, 2007, p. C7.

¹⁵⁷ www.mymobilewatchdog.com

¹⁵⁸ “Radar performed very well and was user-friendly enough for tech-sky parents,” argued Katherine Boehret in a *Wall Street Journal* review of the software. Katherine Boehret, “Keeping Tabs on Kids’ Phones,” *Wall Street Journal*, July 25, 2007. P. D4.

¹⁵⁹ www.wirelessfoundation.org/GetWise/index.cfm

¹⁶⁰ See www.wirelessfoundation.org/GetWise/teachers_guide2007.pdf and www.wirelessfoundation.org/GetWise/family_takehome2007.pdf

¹⁶¹ www.wirelessfoundation.org/GetWise/contest.cfm

2. Mobile Devices Geared toward Younger Users

In addition to the parental controls and screening services offered by carriers, wireless handsets geared specifically for younger children are now on the market.¹⁶² These devices give parents considerable control over what their kids can access on their phones, as well as several other useful monitoring features.¹⁶³ For example:

- Firefly Mobile sells a tiny, voice-only phone for kids with just five buttons on it.¹⁶⁴ Two of the buttons have small icons symbolizing Mom and Dad, allowing the child to call them directly via pre-programmed numbers. It comes in several colors and contains a variety of accessories geared toward kids.
- Another such phone called the TicTalk¹⁶⁵ is marketed by wireless company Enfora and the educational toy maker LeapFrog Enterprises. The TicTalk lets parents enter phone numbers that can be called anytime and also restrict numbers that can be called only during certain times of the day. Parents can also determine what times during the day the phone can even ring.¹⁶⁶
- The Wherify “Wherifone” offers robust GPS location tracking via the Internet. Phone numbers can be programmed by parents and the phone contains an SOS panic button for emergencies. The Wherifone also restricts the downloading of games, as well as text messages.¹⁶⁷
- Guardian Angel Technology also produces a GPS phone for children that lets parents monitor their kids via the Internet.¹⁶⁸ Guardian phones let parents keep a record of their child’s movements for a 30-day period. And when the child is traveling in a car, the phone can monitor how fast the car is going and the direction in which it is heading.

¹⁶² Many of these phones are discussed and sold at www.kidswireless.com

¹⁶³ For more information, see Dan Costa, “Yes, I Spy on My Kid,” *PC Magazine*, July 17, 2007, p. 58, www.pcmag.com/article2/0,1895,2145504,00.asp; Yuki Noguchi, “Connecting with Kids, Wirelessly,” *Washington Post*, July 7, 2005, p. A1; Fern Shen, “Only a Few Can Hear You Now: Limited-Use Phones Geared to Kids,” *Washington Post*, July 18, 2005, p. C14; David Pogue, “Cellphones That Track Kids,” *New York Times*, December 21, 2006, www.nytimes.com/2006/12/21/technology/21pogue.html?ex=1167973200&en=898b8ec6c58ef344&ei=5070;

¹⁶⁴ www.fireflymobile.com

¹⁶⁵ www.mytictalk.com

¹⁶⁶ Kim-Mai Cutler, “A Phone of Their Own,” *Wall Street Journal*, August 4, 2005, p. D1.

¹⁶⁷ www.wherify.com/wherifone

¹⁶⁸ www.guardianangeltech.com

- Verizon Wireless's "Migo" is similar to the Firefly Mobile phone in that has a limited number of buttons for parents to program with approved and emergency-related numbers.¹⁶⁹ Kids can decorate the colorful phone with stickers and other accessories. Using Verizon's Chaperone service, parents can enable GPS tracking of their kids.¹⁷⁰ Verizon also offers a feature called Child Zone which notifies parents via a text message if their child strays beyond pre-approved boundaries.¹⁷¹

3. Independent Mobile Phone Filters

While most parents will likely use the parental control technologies embedded in mobile devices or provided by the network provider, independent mobile phone filtering and monitoring technologies are now coming to market.¹⁷² These filters typically replace the phone's installed web browser with an alternative browser that can't be disabled. That browser then allow parents to configure their child's mobile device in much the same way the parent's would configure filtering software for a child's personal computer.

For example, Safe Eyes Mobile, which retails for \$19.95, lets parents choose from 35 categories to determine what sort of content will be allowed or blocked.¹⁷³ Settings can be changed remotely by parents through a web-based interface. iWonderSurf works in a similar fashion and costs \$14.99.¹⁷⁴ Mobicip, another provider of mobile phone filtering and monitoring, costs \$9.99 for the premium version of its software.¹⁷⁵ Unfortunately, however,

¹⁶⁹ http://estore.vzwshop.com/search/devices/lg_migo.html

¹⁷⁰ www.verizonwireless.com/chaperone

¹⁷¹ www.kidswireless.com/articles/verizon-wireless-chaperone

¹⁷² Jenna Wortham, "Helping Parents Snoop on Kids' iPhone Habits," *New York Times Bits*, March 28, 2009, <http://bits.blogs.nytimes.com/2009/03/28/helping-parents-snoop-on-kids-iphone-habits>

¹⁷³ www.internetsafety.com/safe-eyes-mobile-iphone.php. Also see Michelle Maltais, "Safe Eyes Mobile Puts Parental Controls on iPhone Web Surfing," *Los Angeles Times.com*, March 3, 2009, <http://latimesblogs.latimes.com/technology/2009/03/appiphilia-safe.html>

¹⁷⁴ www.iwondersurf.com

¹⁷⁵ www.mobicip.com

these three filtering tools currently only work with Apple's iPhone, but that will likely change in coming months.

4. Wireless Location-Based Services and Social Mapping

Many of the phones and services described above include location-based technologies that parents can use to monitor the movement of their children.¹⁷⁶ Those same geo-location services can be used for other purposes. Geo-location technologies are now being married to social networking utilities to create an entirely new service and industry: social mapping.¹⁷⁷

Social mapping allows subscribers to find their friends on a digital map and then instantly network with them. Companies such as Loopt,¹⁷⁸ Helio¹⁷⁹ and Google¹⁸⁰ have already rolled out commercial social mapping services. Loopt has also partnered with major carriers Verizon and Sprint to roll out its service nationwide;¹⁸¹ it is also now available on BlackBerry devices and Apple's iPhone. It is likely many other rivals will join them in coming months and years.¹⁸² This new service presents exciting opportunities for users to network with friends and

¹⁷⁶ According to a recent Jupiter Research survey, 4 out of 10 parents with children under age 13 are willing to pay to track their child's location. See "Parents Wants Mobile Phone Kid Tracking," *eMarketer*, August 10, 2007, www.emarketer.com/Article.aspx?id=1005248

¹⁷⁷ "Social networking is just the beginning. Eventually all forms of communication will converge on one pocket-size gizmo that lets you access virtually any information anywhere, at any time. Other people can likewise use their gizmo to find you—as will anyone interested in selling you location-based services. Or you can simply turn off and eat a sub—provided you can resist the urge to broadcast that info to the world." Dan Tynan, "Is That a Social Network in Your Pocket?" *PC World*, August 2007, p. 49. Also see Kate Greene, "The Future of Mobile Social Networking," *Technology Review*, June 2, 2008, www.technologyreview.com/Infotech/20844

¹⁷⁸ <https://loopt.com>

¹⁷⁹ www.helio.com

¹⁸⁰ www.google.com/latitude

¹⁸¹ Amol Sharma and Jessica Vascellaro, "Phones Will Soon Tell Where You Are," *Wall Street Journal*, March 28, 2008, p. A1, <http://online.wsj.com/article/SB120666235472370235.html>

¹⁸² Research firm eMarketer has estimated there were over 63 million location-based service users worldwide in 2008, and that there will be 486 million by 2012. "Mobile Location-Based Services on the Move," *eMarketer*, October 6, 2008, www.emarketer.com/Article.aspx?id=1006609

family, but it might also raise some privacy concerns.¹⁸³ For example, a parent might wonder: “Are random strangers or bad guys monitoring my daughter’s whereabouts? Or, is her former boyfriend using such a service to track and stalk her?”

Industry is responding to these concerns preemptively. As part of their effort to create and refine their “Wireless Content Guidelines,” the CTIA has worked with some of these companies to create privacy and safety guidelines for this emerging technology and industry sector. Loopt, Helio and Google have already taken steps to protect user privacy by establishing a variety of safeguards to ensure that information is not shared inappropriately.¹⁸⁴ Also, tools like Radar and IMSafer can help parents monitor their children’s activities.

These tools and industry best practices will be refined and extended, but they are no substitute for parents talking to their kids about proper use of this new technology.¹⁸⁵ Children need to be educated about how these technologies work and taught to use the tools built into the services to safeguard their personal information. If parents decide to give phones to their pre-teen children, they should configure those phones for them to ensure that these services are disabled or only accessible by trusted family members and acquaintances.

¹⁸³ Laura M. Holson, “Privacy Lost: These Phones Can Find You,” *New York Times*, October 23, 2007, www.nytimes.com/2007/10/23/technology/23mobile.html?_r=2&adxnnl=1&oref=slogin&adxnnlx=1193960357-7mFoDVQXullPWYqVnT/CYA

¹⁸⁴ For Loopt’s safety and privacy tips see: <https://loopt.com/loopt/beSafe.aspx>

¹⁸⁵ The National Institute on Media and the Family produces an excellent guide for parents entitled “Cell Phones and Your Kids” that offers friendly pointers for parents looking to teach their children proper cell phone etiquette. See *A MediaWise Parent Guide—Cell Phones and Your Kids*, (Minneapolis, MN: National Institute on Media and the Family, 2006), www.mediafamily.org/network_pdf/cellphon_guide.pdf Also see: Jan Faull, “Teaching Kids Cell Phone Etiquette,” *MSN Lifestyle*, August 2006, <http://lifestyle.msn.com/FamilyandParenting/RaisingKids/ArticleBHG.aspx?cp-documentid=1314613>; “Cell Phone Safety Tips,” *ConnectSafely.org*, www.connectsafely.org/safety-tips/safety-tips/cell-phone-safety-tips.html

F. Internet & Social Networking Sites

The staggering scale of the Internet and the sheer scope and volume of online activities make parental control efforts quite challenging. That's especially the case because, as the Pew Internet & American Life Project notes, "American teens are more wired now than ever before."¹⁸⁶

Luckily, many companies and private organizations have already established tools and methods to deal with objectionable online content. Parents need to adopt a "layered" approach to online child protection that involves many of the tools and strategies outlined in this section. An excellent illustration of how this works is found in Gregory S. Smith's *How to Protect Your Children on the Internet: A Road Map for Parents and Teachers*.¹⁸⁷ The adjoining exhibit depicts the 8-part layered model Smith outlines in his book to help parents and teachers keep kids safe online.

Of course, it goes without saying that these methods should not be considered substitutes for talking to children about what they might see or hear while online. Even though the tools and strategies that follow can help parents control the vast majority of objectionable content that their kids might stumble upon while online, no one system is perfect. In the end, education, oversight, and ongoing communication and mentoring are vital.¹⁸⁸ That being said,

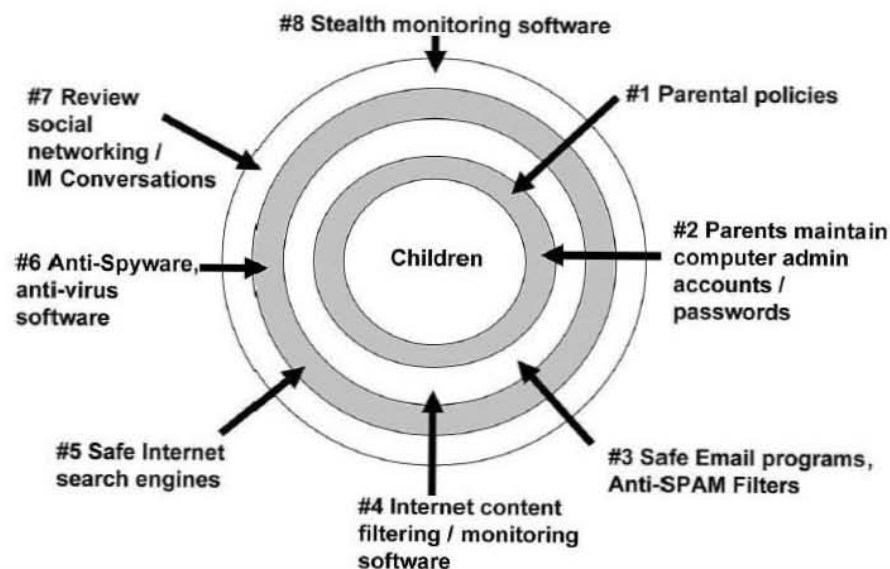
¹⁸⁶ Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew Internet & American Life Project, April 18, 2007, p. 3, www.pewinternet.org/PPF/r/211/report_display.asp

¹⁸⁷ Gregory S. Smith, *How to Protect Your Children on the Internet: A Road Map for Parents and Teachers* (Westport, CT: Praeger, 2007), p. 72, www.gregoryssmith.com

¹⁸⁸ Julia Angwin of the *Wall Street Journal* argues: "For most parents, it seems that our best bet is to treat the Internet like an unsupervised playground in a sketchy neighborhood: You shouldn't drop your kids off there and walk away. You are obligated to stick around and make sure some kid doesn't beat up your kid – even if you're just watching from a bench on the sidelines." Julia Angwin, "How to Keep Kids Safe Online," *Wall Street Journal*, January 20, 2009, <http://online.wsj.com/article/SB123238632055894993.html>

there are many tools and strategies that can be an important part of the “training wheels and speed bumps” approach discussed in Section I.

Exhibit 30:
Gregory Smith’s 8-Step Plan to Protect Children from Online Risks



1. Filters and Monitoring Software

One of the first things that most of these sites and books recommend is that parents install filtering or monitoring software on the computers their children use. Parents can either use “client-side” filtering and monitoring tools or rely on the parental control tools provided by their Internet service provider, often called “server-side” controls. A discussion of both types of tools follows.

a) Independent / “Client-Side” Filters and Monitoring Tools:

Most parents are familiar with Internet filtering software and many parents use filters to control their children’s online surfing activities. Until recently, most filtering software was purchased at retail stores or downloaded from websites and installed on the user’s personal computer. These stand-alone or “boxed” filtering solutions are typically referred to as “client-

side” filters. These client-side solutions are still very popular and, as Exhibit 38 illustrates, many different vendors continue to compete in this market.¹⁸⁹

At a minimum, these software tools let parents block access to adult websites and typically let parents impose time management constraints on their children’s computer and Internet usage. Increasingly, however, these software packages also include far more robust monitoring tools that let parents see each website their children visit, view every e-mail or instant message that they send and receive, or even record every word that they type into their word processors.¹⁹⁰ Many of these stealth monitoring tools can then send parents a periodic report summarizing their child’s Internet usage and communications. More robust software programs even allow parents to capture screen shots of sites their kids have visited. Finally, these tools allow parents to do all this in a surreptitious fashion since, once the software is installed on a child’s computer, it is entirely invisible to the child user.

Many of these tools include e-mail monitoring capabilities and some are exclusively tailored to ensuring child-friendly e-mail experiences. For example, ZooBuh lets parents approve their child’s e-mail contact list and manage file attachments.¹⁹¹ It also has a “bad words” filter to block foul language and parents can add specific words to the system they want to see blocked. AOL and Microsoft have similar capabilities built into their family safety offerings.

¹⁸⁹ A comprehensive list of filter providers can be found on David Burt’s “Filtering Facts” blog: <http://filteringfacts.org/filtering/filtering-companies/>

¹⁹⁰ See Jessica E. Vascellaro and Anjali Athavaley, “Foley Scandal Turns Parents Into Web Sleuths,” *Wall Street Journal*, October 18, 2006, p. D1.

¹⁹¹ www.zoobuh.com

Exhibit 31: Internet Filtering and Monitoring Software for PCs

- AOL Parental Controls (<http://parentalcontrols.aol.com>)
- BeNetSafe (www.benetsafe.com)
- Bsafe Online (<http://bsafeonline.com>)
- Clean Internet.com (<http://cleaninternet.com>)
- Content Cleaner (www.contentpurity.com)
- CyberPatrol (www.cyberpatrol.com)
- Cyber Sentinel (www.cybersentinel.com)
- CyberSitter (www.cybersitter.com)
- eBlaster (www.spectorsoft.com)
- FamLink (www.familink.com)
- Family Cyber Alert (www.itcompany.com)
- FilterGate (<http://filtergate.com>)
- FilterPak (www.surfguardian.net/products.shtml)
- Guardian Monitor (www.guardiansoftware.com)
- IamBigBrother (www.iambigbrother.com)
- iShield (www.guardwareinc.com)
- K9 Web Protection (www.k9webprotection.com)
- KidsNet (www.kidsnet.com)
- Livia Web Protection (www.liviaweb.com)
- McAfee Internet Security Suite (<http://us.mcafee.com>)
- McGruff SafeGuard (www.GoMcGruff.com)
- Microsoft Live One Care (www.windowsoncare.com)
- Miss America Kid Safe Web Browser (www.missamericakids.com)
- NetIntelligence (www.netintelligence.com)
- Netsweeper (www.netsweeper.com)
- NetMop (www.netmop.com)
- NetNanny (www.netnanny.com)
- NoodleNet (www.noodlenet.com)
- Norton Internet Security (www.symantec.com/home_homeoffice/products)
- Online Safety Shield (www.onlinesafetyshield.com)
- Optenet PC (www.optenetpc.com)
- Parental Control Bar (www.wraac.org)
- PC Pandora (www.pcpandora.com)
- PC Tattletale (www.pctattletale.com)
- Razzul (www.kidinnovation.com)
- SafeEyes (www.internetsafety.com/safe-eyes)
- SafeSquid (www.safesquid.com)
- Sentry At Home (www.sentryparentalcontrols.com)
- Sentry Remote (www.sentryparentalcontrols.com)
- SnoopStick (www.snoopstick.com)
- Spector Pro (www.spectorsoft.com)
- SoftActivity Keylogger (www.softactivity.com)
- Spy Agent (www.spytech-web.com/software.shtml)
- Surf On the Safe Side (www.surfonthesafeside.com)
- SurfPass (www.cogilab.com)
- Surf Recon (www.surfrecon.com)
- Webroot Parental Controls (www.webroot.com)
- WebWatcher (www.awarenesstech.com/parents/index.html)

Similarly, IMSafer offers a free downloadable tool that can help parents monitor instant messenger conversations and notify them when their child is engaged in a potentially dangerous conversation on IM.¹⁹² Importantly, the IMSafer tool respects a child's privacy since parents are not allowed to read the full transcripts of online communications. Instead, the application only monitors IM conversations for content that is considered dangerous. Importantly, however, this includes the trading of phone numbers or other personal information. Safe Chat Universal Messenger works much the same way, letting parents block foul language or specific sites and users on various IM networks, such as MSN, Yahoo, AIM, and ICQ.¹⁹³

Some parents might flinch at this level of child surveillance, but others will find it entirely appropriate, especially for very young children just getting online.¹⁹⁴ Regardless, a wide variety of such filtering and monitoring tools is available and they can be calibrated to meet parents' specific needs and values. A comprehensive list of these software tools can be found at the GetNetWise.org website,¹⁹⁵ and some of the most popular filtering and monitoring tools are listed in the adjoining exhibit. Of course, not all filtering and monitoring tools are equal, and features vary by product. Moreover, tools come and go, and many change over time in terms of functions and capabilities.

¹⁹² www.imsafer.com

¹⁹³ hwww.zihtec.com/en/how_safe_chat_protects_children.html

¹⁹⁴ As the National Research Council report concluded of monitoring software: "[A]ctive supervision of children is often appropriate—not because they are criminals but because it is the responsibility of adults to teach them how to internalize the appropriate values and to become better at avoiding inappropriate behavior as they mature." Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), p. 315.

¹⁹⁵ See www.getnetwise.org

Exhibit 32: Filter and Monitoring Software Review Sites

- www.child-internet-safety.com
- www.monitoringsoftwarereviews.org
- <http://filteringfacts.org/filtering/filtering-companies>
- <http://internet-filter-review.toptenreviews.com>
- www.filterreview.com
- www.download.com/sort/3150-2162_4-0-1-3.html
- www.consumersearch.com/www/software/parental-control-software/index.html
- www.pcmag.com/category2/0,1874,1639158,00.asp

What's important for parents to keep in mind is that these two types of tools are complementary. On their own, neither tool is perfect. When used in combination, however, they provide parents a formidable set of tools to better control their children's online activities.

As Gregory Smith, author of *How to Protect Your Children on the Internet*, notes:

Content filtering and monitoring software has come a long way in the past few years and is getting more powerful with every new release. That said, it's by no means perfect and should not be the only technical solution that adults rely on to ensure that their kids are doing the right things and are not putting themselves at risk by posting personal information or conversing with strangers in cyberspace. That's where stealth software... comes into play. It removes any doubt about what your children are doing on the Internet by providing the clear facts of their online habits, tools, and even with whom they are conversing, regardless of the tool used. Stealth software also fills in the gaps that imperfect content filtering solutions have in the marketplace.¹⁹⁶

b) *ISP-Integrated ("Server-Side") Parental Controls and Filtering Tools:*

Stand-alone or "client-side" filtering solutions, such as those described above, dominated the online parental controls marketplace in the late 1990s. The market has changed significantly since then, however. Today, Internet service providers (ISPs)—including major

¹⁹⁶ Gregory S. Smith, *How to Protect Your Children on the Internet: A Road Map for Parents and Teachers* (Westport, CT: Praeger, 2007), p.97-99.

broadband service providers (BSPs)—offer parental control services as part of an integrated suite of security tools, which typically include anti-virus, anti-spyware, and anti-Spam tools.

Exhibit 33:
Internet Security and Parental Control Websites
for Major ISPs and Broadband Operators

- AOL (<http://daol.aol.com/security>)
- AT&T (www.att.com/smartlimits) + (www.att.com/safety)
- Cablevision (www.powertolearn.com/internet_smarts/index.shtml)
- Charter (www.charter.com/Visitors/NonProducts.aspx?NonProductItem=65)
- Comcast (www.comcast.net/security)
- Cox (www.cox.com/takecharge/internet_controls.asp)
- Earthlink (www.earthlink.net/software/free/parentalcontrols)
- Insight BB (www.insightbb.com/pcsecurity/default.aspx)
- Microsoft (www.microsoft.com/protect)
- NetZero (www.netzero.net/support/security/tools/parental-controls.html)
- Qwest (www.incredibleinternet.com)
- Time Warner (www.timewarnercable.com)
- Verizon (<http://parentalcenter.verizon.radialpoint.net>)

These security options are often offered free of charge, or for a small additional fee, when subscribers sign up for monthly Internet service. And most of these integrated tools offer automatic updates such that consumers need not manually download upgrades to stay current. Thus, millions of parents now have free or quite inexpensive Internet parental control tools at their disposal as soon as they sign up for Internet access through an ISP. Of course, parents can also add on other tools or independent filtering and monitoring solutions such as those outlined earlier. The adjoining exhibit lists the Internet security websites for major ISPs and broadband operators and provides screen shots of some of their websites.

Exhibit 34: Major ISP Online Safety Sites

AT&T's "Smart Limits"



Qwest's "Incredible Internet"



NCTA's "Point Smart. Click Safe"



Verizon's "Parental Control Center"



2. Operating Systems and Web Browser Controls

Increasingly, companies like Microsoft and Apple are integrating parental controls into computer operating systems and web browsers. As Walter Mossberg of *The Wall Street Journal* notes, these are “powerful tools to help parents get a handle on their children’s computing and online activities.”¹⁹⁷ “The battle to one-up each other in parental controls is only going to benefit consumers,” said Chris Swenson, director of software industry analysis at the research

¹⁹⁷ Walter S. Mossberg, “You Have Weapons in Your Computer to Monitor Your Kids,” *Wall Street Journal*, June 14, 2007, p. B1.

firm the NPD Group. “There’s really no excuse now for parents not to lock down their PCs for their children.”¹⁹⁸

a) *Microsoft’s “Vista” OS and Internet Explorer browser:*

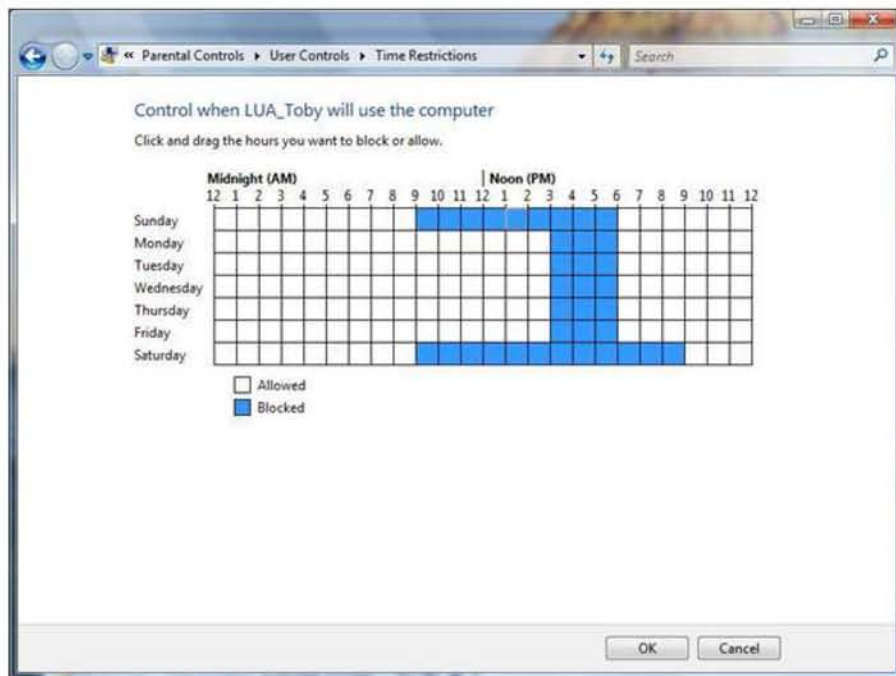
Released in 2007, the Windows Vista operating system is Microsoft’s first version of Windows that incorporates embedded family safety tools. As Seth Schiesel of *The New York Times* reports, “With Vista, Microsoft has for the first time built a robust set of parental controls directly into the operating system, not just for gaming but also for Web browsing, file downloading and instant messaging.”¹⁹⁹

Vista lets parents establish “administrator” accounts and then oversee the individual users—namely, their own children—who are using the PCs. Parents can then configure the Vista sub-accounts to enable various parental control features and monitoring tools. They can turn on web filters that will block specific types of potentially objectionable website content or downloads. Time limits can also be established for the PC that restrict when or how long the child may use the computer.

¹⁹⁸ Quoted in Stefanie Olsen, “Parents the Winner in Leopard, Vista Showdown,” *CNet News.com*, November 20, 2007, www.news.com/Parents-the-winner-in-Leopard%2C-Vista-showdown/2009-1025_3-6219420.html

¹⁹⁹ Seth Schiesel, “For Parents, New Ways to Control the Action,” *New York Times*, January 8, 2007, www.nytimes.com/2007/01/08/arts/08vist.html?ex=1325912400&en=3bb7bc1b6a470a23&ei=5090&partner=rssuserland&emc=rss

Exhibit 35: Vista Operating System Parental Controls



Also, much like new video game consoles, Vista will also let parents restrict video game play by rating or title, or entirely block games with no ratings. Parents can also see an “activity list” of the sites their child has visited, or attempted to visit, as well as files and applications that have been downloaded. Applications or software parents find objectionable can then be

blocked from that same screen.²⁰⁰ Importantly, once these parental controls have been enabled within Vista, there is no need for parents to configure additional controls within Internet Explorer. Vista controls all Internet Explorer web-browsing activities.

Finally, Microsoft has opened up “application programming interfaces” (APIs) to third-party software developers so that they can build additional parental control tools on top of Vista. One of these developers is IMSafer, which was discussed earlier. A number of other add-ons for Internet Explorer let parents add further layers of controls.

b) Apple’s OS X “Leopard” and Safari browser:

With Apple’s recent release of its OS X “Leopard” operating system, the company’s parental control tools have grown more sophisticated and rival Microsoft’s Vista-based controls.²⁰¹

Apple’s operating system allows parents to establish accounts for their children and keep tabs on their online activities using monitoring tools and time management controls. In addition, parents can also build a restricted “buddies list” for their children and then disallow instant messaging to anyone else. The system can also hide the child’s online status so that only those pre-approved buddies can see that they are online at any time.

Apple’s Safari web browser works in conjunction with the Leopard filter to maintain a safe online experience. Parents can establish whitelists of websites their children can visit, thus blacklisting sites not on the list.

²⁰⁰ www.microsoft.com/windowsvista/features/forhome/safety.msp#more

²⁰¹ www.apple.com/macosx/features/parentalcontrols.html

Exhibit 36:
“Glubble” for the Firefox Web Browser



c) Firefox / Glubble:

Firefox is an independent web browser managed by the non-profit Mozilla Foundation. Although Mozilla does not offer parental controls directly for the Firefox browser, third parties are free to devise and offer parental control tools as “add-ons” to the browser. “Glubble” is one such example.²⁰² Once the program is loaded onto a user’s computer, Glubble locks the Firefox browser such that a password is required before a user can access the Internet. Parents can then establish a user account for their children that allows them access only to a set of pre-screened, kid-friendly websites.

d) KidZui:

KidZui is a kid-friendly browser that works with both Windows and Apple-based operating systems.²⁰³ As of October 2008, the service was providing access to over 1.5 million kid-friendly websites, videos, and pictures that had all been pre-screened by over 200 trained

²⁰² www.glubble.com

²⁰³ www.kidzui.com

teachers and parents.²⁰⁴ The company employs a rigorous 5-step “content selection process” to determine if it is acceptable for kids between 3-12 years of age.²⁰⁵ Parents are also sent an activity report for their child to see what they have been viewing. The service costs \$39.95/year, or \$7.95/month to access all services, but a stripped-down version of the software is also available for free.²⁰⁶

Exhibit 37: KidZui Web Browser



²⁰⁴ www.marketwire.com/press-release/Kidzui-909109.html

²⁰⁵ www.kidzui.com/contentselection

²⁰⁶ For an independent review of the KidZui service, see: Walter Mossberg, “KidZui’s Parent Plan Lets Children Explore in Safe Corner of Web,” *Wall Street Journal*, March 20, 2008, p. B1, http://online.wsj.com/article/SB120597536349250547.html?mod=technology_featured_stories_hs; Amy Tiemann, “Kidzui Creates a New Online Environment for Kids,” *CNet News*, ParentThesis, March 20, 2008, www.cnet.com/8301-13507_1-9900282-18.html

e) *Other “Child-Safe” Browsers:*

There are other kid-friendly browsers that operate much like KidZui and Glubble, including Peanut Butter PC,²⁰⁷ Noodle Net,²⁰⁸ and the Hoopah Kidview Computer Explorer.²⁰⁹ Neil Rubenking of *PC Mag.com* notes that “Child-safe browsers strip away a lot of the complexity of Internet Explorer or Firefox. They generally block pop-ups, allow only one page to be open at a time, and suppress confusing right-click menus. Typically you’ll find just a few big buttons—perhaps just a Home and a Back button. And they limit the sites kids can visit.” These browsers also lock children out of the rest of mom and dad’s PC so that they cannot access or delete important files on the hard drive.²¹⁰

3. “Safe Search” Engine Filters and Web Portals for Kids

Parents can also use tools embedded in search engines to block a great deal of potentially objectionable content that children might inadvertently stumble upon during searches. For example, Google offers a SafeSearch feature that allows users to filter unwanted content. Users can customize their SafeSearch settings by clicking on the “Preferences” link to the right of the search box on the Google.com home page.²¹¹ Users can choose “moderate filtering,” which “excludes most explicit images from Google Image Search results but doesn’t filter ordinary web search results,” or “strict filtering,” which applies the SafeSearch filtering controls to all search engine results.

²⁰⁷ www.peanutbuttersoftware.com

²⁰⁸ www.noodlenet.com

²⁰⁹ www.hoopah.com

²¹⁰ See Neil J. Rubenking, “Child-Safe Browsers,” *PC Mag.com*, July 15, 2008, www.pcmag.com/article2/0,2817,2325581,00.asp.

²¹¹ www.google.com/intl/en/help/customize.html#safe

Exhibit 38: “Safe Search” Filtering Tools

Google

The screenshot shows the Google Help Center page for Search Preferences. On the left is a navigation menu with links like Google Home, About Google, Help Center, Search Guides, Search Features, and Services & Tools. The main content area is titled 'Search Preferences' and explains that users can customize their search. It lists four settings: SafeSearch filtering, Number of results, Language options, and New results window. The 'SafeSearch filtering' section is expanded, showing three options: Moderate filtering (the default), Strict filtering, and No Filtering. It also includes a 'SafeSearch lock' section and a note about the advisory nature of the filtering.

Google

Google Help Center

Google Home
About Google
Help Center
Search Guides
Search Features
Services & Tools

Search Preferences

We want your web search to be exactly the way you want it. Here's a quick review of the search options you can set (and, of course, revise whenever you like) on your [Google Preferences](#) page.

- [SafeSearch filtering](#)
- [Number of results](#)
- [Language options](#)
- [New results window](#)

SafeSearch filtering

Many users prefer not to have adult sites included in search results (especially if their kids use the same computer). Google's SafeSearch screens for sites that contain explicit sexual content and deletes them from your search results. No filter is 100% accurate, but SafeSearch should eliminate most inappropriate material.

You can choose from among three SafeSearch settings:

- **Moderate filtering** excludes most explicit images from Google Image Search results but doesn't filter ordinary web search results. This is your default SafeSearch setting; you'll receive moderate filtering unless you change it.
- **Strict filtering** applies SafeSearch filtering to all your search results (i.e., both image search and ordinary web search).
- **No Filtering**, as you've probably figured out, turns off SafeSearch filtering completely.

You can also adjust your SafeSearch settings on the [Advanced Search](#) or the [Advanced Image Search](#) pages on a per search basis.

We do our best to keep SafeSearch as up-to-date and comprehensive as possible, but inappropriate sites will sometimes slip through the cracks. If you have SafeSearch activated and still find websites containing offensive content in your results, please [contact us](#) and we'll investigate it.

Yahoo!

The screenshot shows the Yahoo! Search Preferences page. It has a header with the Yahoo! logo and a welcome message for 'adam_thierer'. The 'Search Preferences' section is highlighted. Under 'Safe Search', there are 'Save' and 'Cancel' buttons. The 'SafeSearch Filter' section shows three radio button options: 'Filter out adult Web, video, and image search results - SafeSearch On' (selected), 'Filter out adult video and image search results only - SafeSearch On', and 'Do not filter results (results may include adult content) - SafeSearch Off'. The 'SafeSearch lock' section has a checked checkbox for 'Lock SafeSearch setting to filter out adult Web, video, and image search results'. A note and an advisory statement are also present.

YAHOO! SEARCH

Welcome, [adam_thierer](#) [Sign Out](#) - [Yahoo!](#) - [Search Home](#) - [Help](#)

Search Preferences

Safe Search [Save](#) [Cancel](#)

SafeSearch Filter

Applies when I'm signed in:

- ☒ Filter out adult Web, video, and image search results - *SafeSearch On*
- ☐ Filter out adult video and image search results only - *SafeSearch On*
- ☐ Do not filter results (results may include adult content) - *SafeSearch Off*

SafeSearch lock

Applies when anyone using this computer is signed out or signed in as under 18:

- ☒ Lock SafeSearch setting to filter out adult Web, video, and image search results

Note: Any user signed in on your computer as 18 or older can change this setting. We recommend periodically checking the SafeSearch Lock settings.

Advisory: Yahoo! SafeSearch is designed to filter out explicit, adult-oriented content from Yahoo! Search results. However, Yahoo! cannot guarantee that all explicit content will be filtered out.

[Learn more](#) about protecting children online.

Microsoft

The screenshot shows the Microsoft Live Search preferences page. It has a header with the 'Live Search' logo and a search bar. The 'Display' section has a dropdown menu set to 'English'. The 'Results' section has a 'Show' dropdown set to '10' and checkboxes for 'Group results from the same site' (checked) and 'Open links in a new browser window'. The 'SafeSearch' section has three radio button options: 'Strict' (selected), 'Moderate', and 'Off'. A note at the bottom explains that the system is not 100% accurate.

Live Search

Display Customize the search display.

Display this site in [English](#)

Results Choose how your results appear.

Show [10](#) results on each page

- ☒ Group results from the same site. Show the first [2](#) results.
- ☐ Open links in a new browser window

SafeSearch Choose how you want to filter results.

- ☒ Strict - Filter sexually explicit text results. Filter sexually explicit images using strict filtering.
- ☐ Moderate - Do not filter text results. Filter sexually explicit images using moderate filtering.
- ☐ Off - Do not filter search results.

Note: Although SafeSearch uses advanced technology to filter sexually explicit content, no system of this type can be 100% accurate. We cannot guarantee that all sexually explicit content will be excluded. [Learn more about filtering offensive sites.](#)

Location Set your default location.

Similarly, Yahoo! has a SafeSearch tool that can be found under the “Preferences” link on the “My Web” tab.²¹² Like Google, Yahoo! allows strict or moderate filtering. Microsoft’s Live Search works largely the same way.²¹³ Other search engine providers such as AltaVista,²¹⁴ AskJeeves,²¹⁵ HotBot,²¹⁶ Lycos,²¹⁷ and AllTheWeb,²¹⁸ also provide filtering tools. Working in conjunction with other filters, these search engine tools are quite effective in blocking a significant amount of potentially objectionable content.

Exhibit 39: Kid-Friendly Internet Search Engines and Web Portals

- ALA’s Great Web Sites for Kids (www.ala.org/greatsites)
- AOL for Kids (U.S.) (<http://kids.aol.com>)
- AOL for Kids (Canada) (<http://canada.aol.com/aolforkids>)
- Ask Kids (www.askkids.com)
- Awesome Library for Kids (www.awesomelibrary.org)
- Diddabadoo (www.dibdabadoo.com)
- Education World (www.education-world.com)
- Fact Monster (www.factmonster.com)
- FirstGov for Kids (www.kids.gov)
- KidsClick (www.kidsclick.org)
- Kid Zui (www.kidzui.com)
- Noodle Net (www.noodlenet.com)
- NetTrekker (www.nettrekker.com)
- SearchEdu.com (www.searchedu.com)
- Surfing the Net with Kids (www.surfnetkids.com)
- TekMom’s Search Tools for Students (www.tekmom.com/search)
- ThinkQuest (www.thinkquest.org)
- Yahoo! Kids (<http://kids.yahoo.com>)

²¹² <http://myweb.yahoo.com>

²¹³ <http://search.msn.com/settings.aspx>

²¹⁴ www.altavista.com/web/ffset?ref=/

²¹⁵ www.ask.com/webprefs

²¹⁶ www.hotbot.com/prefs_filters.asp

²¹⁷ <http://search.lycos.com/adv.php?query=&adf=>

²¹⁸ www.alltheweb.com/customize?backurl=Lw&withjs=1

A better approach to use with younger children is to direct them to search engines or web portals geared toward younger audiences. Several excellent websites, such as those listed in an adjoining exhibit, let kids search numerous sites without stumbling upon adult-oriented material,²¹⁹—or, better yet, direct children to sites and information that are educational and enriching. In essence, these search portals are massive whitelists of acceptable sites and content that have been pre-screened to ensure that they are appropriate for very young web surfers. The only downside of using such services is that a lot of wonderful material available on the World Wide Web might be missed, but many parents will be willing to make that trade-off since they desire greater protection of their children from potentially objectionable content.

4. More Online Content-Tailoring Options and Kid-Friendly Websites

The child-friendly web portals discussed above generally direct children to informational and educational sites and resources. There are many other ways to tailor the web-surfing experience to a family's specific needs and values. The Internet is full of wonderful sites dedicated to kids and teens. Many have an educational focus, whereas others offer enjoyable games and activities for children. The adjoining exhibit highlights some of the best of these websites, but this list only scratches the surface. If parents wanted, they could configure their web browsers to access only sites such as these and then block access to all other webpages.

²¹⁹

This lists builds on the excellent compendium of sites listed at the Search Engine Watch website: <http://searchenginewatch.com/showPage.html?page=2156191>

Exhibit 40: Child- and Teen-Oriented Websites & Virtual Worlds

- Candy Stand (www.candystand.com)
- Clever Island (www.cleverisland.com)
- Club Penguin (www.clubpenguin.com)
- Disney's Club Blast (<http://disney.go.com/blast>)
- Disney's DGamer (<http://disney.go.com/dxd2/index.html?channel=68447>)
- Disney's Playhouse (<http://disney.go.com/playhouse/today/index.html>)
- Disney Toontown Online (<http://play.toontown.com>)
- Everything Girl (<http://pollypocket.everythinggirl.com>)
- Fun Brain (www.funbrain.com)
- Habbo (www.habbo.com)
- HBO Family Games (www.hbofamily.com/games)
- Iland5 (www.iland5.com)
- Kaboose Family Network (www.kaboose.com)
- Kaboose FunSchool (<http://funschool.kaboose.com>)
- KidsClick (www.kidsclick.org)
- KidsFirst (www.kidsfirst.org)
- NeoPets (www.neopets.com)
- Net Smartz Kids (www.netsmartzkids.org)
- Nickelodeon Games (www.nick.com/games)
- Nick Jr. Playtime (www.nickjr.com/playtime)
- Nicktropolis (www.nicktropolis.com)
- Noggin Games (www.noggin.com/games)
- PopCap (www.popcap.com)
- PBS Kids (<http://pbskids.org/go>)
- Surfing the Net with Kids (www.surfnetkids.com)
- Webkinz (www.webkinz.com)
- Yahoo! Kids (<http://kids.yahoo.com>)
- YoKidsYo (www.yokidsyo.com)
- Zeeks (www.zeeks.com)
- Zoey's Room (www.zoey'sroom.com)
- Zwinky Cuties (www.zwinkycuties.com)

5. Social Networking Site Safety & Cyberbullying Concerns

Social networking websites have become wildly popular with teenagers in recent years. Sites such as MySpace, Facebook, Xanga, Bebo, LiveJournal, and Windows Live Spaces attract millions of users and represent just a few of the hundreds of social networking sites (SNS) online today.²²⁰ These sites offer their users the space and tools to build the equivalent of an online journal and to easily network with others. It seems that new sites surface every week,

²²⁰

For a list of notable social networking sites, see:
http://en.wikipedia.org/wiki/List_of_social_networking_websites

growing ever-more personalized in an attempt to appeal to specific niches.²²¹ Social networking services are also being integrated into gaming consoles, and many video games increasingly feature interactive social networking features.²²²

Many parents and policymakers have grown quite concerned about how youngsters use these social networking sites and services. These concerns have prompted lawmakers to introduce legislation to ban access to such sites in schools and libraries.²²³ Others, including several state attorneys general, want such sites to age-verify all users to exclude those over or under a certain age.²²⁴ The limitations and dangers of mandatory age verification schemes are discussed in more detail in Section V.²²⁵

These concerns are not surprising. “People naturally fear what they do not understand,” says Jason Illian, author of *MySpace, MyKids*.²²⁶ But, “regardless of how you feel about the Internet and online communities, they are here to stay... Likewise, we’re not going to stop our

²²¹ See Robert D. Hof, “There’s Not Enough ‘Me’ in MySpace,” *Business Week*, December 4, 2006, p. 40.

²²² Walaika Haskins, “Gamin’s Play for Social Networks,” *Tech News World*, May 12, 2008, www.technewsworld.com/story/social-networking/62953.html

²²³ In the 109th Congress, former Rep. Michael Fitzpatrick (R-PA) introduced the Deleting Online Predators Act (DOPA), which proposed a ban on social networking sites in public schools and libraries. DOPA passed the House of Representatives shortly thereafter by a lopsided 410-15 vote, but failed to pass the Senate. The measure was reintroduced just a few weeks into the 110th Congress by Senator Ted Stevens (R-AK), the ranking minority member and former chairman of the Senate Commerce Committee. It was section 2 of a bill that Sen. Stevens sponsored titled the “Protecting Children in the 21st Century Act” (S. 49). See Declan McCullagh, “Chat Rooms Could Face Expulsion,” *CNet News.com*, July 28, 2006, http://news.com.com/2100-1028_3-6099414.html?part=rss&tag=6099414&subj=news; Anne Broache, “Congress Off to Slow Start with Tech,” *ZDNet News*, January 9, 2007, http://news.zdnet.com/2100-9588_22-6148312.html

²²⁴ Susan Haigh, “Conn. Bill Would Force MySpace Age Check,” *Yahoo News.com*, March 7, 2007, www.msnbc.msn.com/id/17502005

²²⁵ Also see Adam Thierer, “Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,” Progress & Freedom Foundation *Progress on Point* 14.5, March 21, 2007. www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf

²²⁶ Jason Illian, *MySpace, MyKids* (Eugene, OR: Harvest House Publishers, 2007), p. 10.

teenagers from chatting online and meeting new people. We just need to teach them how to do it properly so that they don't get hurt."²²⁷

To begin, parents need to understand social networking websites, quite unlike other "professional" websites, feature a great deal of "amateur" user-generated content. This makes it more difficult for filters or other parental control tools to screen out potentially undesirable material. Fortunately, most mainstream social networking sites take steps to pre-screen many of the images that are uploaded to their sites and to block objectionable material. But it will be impossible for website operators to control everything that is said or posted in light of the sheer volume of material and user-to-user communication taking place.

Parents will need to determine which social networking sites are right for their children. As the SNS marketplace evolves and grows, niche SNSes are developing that are tailored to specific age groups or interests. Parents of pre-teens should be particularly careful about letting their kids go on social networking sites. But there are some smaller social networking sites or virtual worlds such as ClubPenguin,²²⁸ Zoey'sRoom,²²⁹ and Nicktropolis²³⁰ that have extremely strict membership policies, primarily because they target or allow younger users.²³¹ Some of these sites also tightly limit chat capabilities to ensure added safety.²³² Parents could also use the "walled garden" browser tools like Glubble and KidZui, which were highlighted above.

²²⁷ *Id.*, p. 11.

²²⁸ www.clubpenguin.com

²²⁹ www.zoey'sroom.com

²³⁰ www.nicktropolis.com

²³¹ A comprehensive list of such sites is available from Virtual Worlds Management: www.virtualworldsmanagement.com/2008/youthworlds.html

²³² Mike Musgrove, "Kid e-Land," *Washington Post*, May 16, 2008, p. D1, www.washingtonpost.com/wp-dyn/content/article/2008/05/15/AR2008051503762.html

Exhibit 41:

MySpace.com's Safety & Security Website



Parents of tweens and teens will need to consider additional solutions once their kids grow tired of those sites and service and want to move on to more mainstream social networking sites. Monitoring software could certainly be part of the answer. Many monitoring tools, discussed earlier, give parents a clear idea of how much time their kids spend online, the specific sites they are visiting, and with whom they are conversing. In January 2008, MySpace.com announced a major agreement with 49 state Attorneys General aimed at better protecting children online.²³³ As part of that agreement, MySpace pledged to take various steps

²³³

Anne Barnard, "MySpace Agrees to Lead Fight to Stop Sex Predators," *New York Times*, January 15, 2008, www.nytimes.com/2008/01/15/us/15myspace.html?ref=us. Also see Adam Thierer, "The MySpace-AG Agreement: A Model Code of Conduct for Social Networking?" Progress & Freedom Foundation *Progress on Point* 15.1, January 2008, www.pff.org/issues-pubs/pops/pop15.1myspaceAGagreement.pdf

to enhance site safety and privacy.²³⁴ Facebook.com struck a similar agreement with AGs following MySpace's pledge.

Additional tips for parents about social networking sites can be found in two very accessible booklets: *MySpace Unraveled: A Parent's Guide to Teen Social Networking*, by Larry Magid and Anne Collier²³⁵ and *MySpace, MyKids*, by Jason Illian.²³⁶ Also, the Federal Trade Commission's OnGuardOnline.gov website offers "Social Networking Safety Tips for Tweens and Teens" as well as "A Parent's Guide" to social networking sites.²³⁷ And the Federal Bureau of Investigation offers "A Parent's Guide to Internet Safety" on its website, with similar advice.²³⁸ MySpace.com also offers safety tips for kids and parents on its site,²³⁹ which includes an "Official Parent and Family Guide" to help them understand how to keep their kids safe online.²⁴⁰ GetNetWise.org also offers excellent step-by-step video tutorials about how to establish privacy settings on major social networking sites to keep your online activities more private.²⁴¹

²³⁴ "MySpace and Attorneys General Announce Joint Effort to Promote Industry-Wide Internet Safety Principles," News Corp. *Press Release*, January 14, 2008, www.newscorp.com/news/news_363.html

²³⁵ Larry Magid and Anne Collier, *MySpace Unraveled: A Parent's Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), p. 2, www.myspaceunraveled.com.

²³⁶ Jason Illian, *MySpace, MyKids* (Eugene, OR: Harvest House Publishers, 2007).

²³⁷ http://onguardonline.gov/socialnetworking_youth.html and <http://onguardonline.gov/socialnetworking.html>

²³⁸ www.fbi.gov/publications/pguide/pguidee.htm

²³⁹ www.myspace.com/Modules/Common/Pages/SafetyTips.aspx

²⁴⁰ "The Official Parent and Family Guide," MySpace.com, <http://cms.myspacecdn.com/cms/SafetySite/documents/MySpaceParentGuide.pdf>

²⁴¹ <http://kids.getnetwise.org/safetyguide/technology/socialnetworking>

Parents should realize that social networks offer them a “window into the world” their kids inhabit. As Jason Illian notes of MySpace, but is also true of all other social networking sites and activities in which our kids engage:

Believe it or not, MySpace can be a great tool for parents. It can be a second pair of eyes and ears for those who want to better understand their children and the challenges they face. Parents can use this virtual community to monitor, interact with, and encourage their kids like never before.

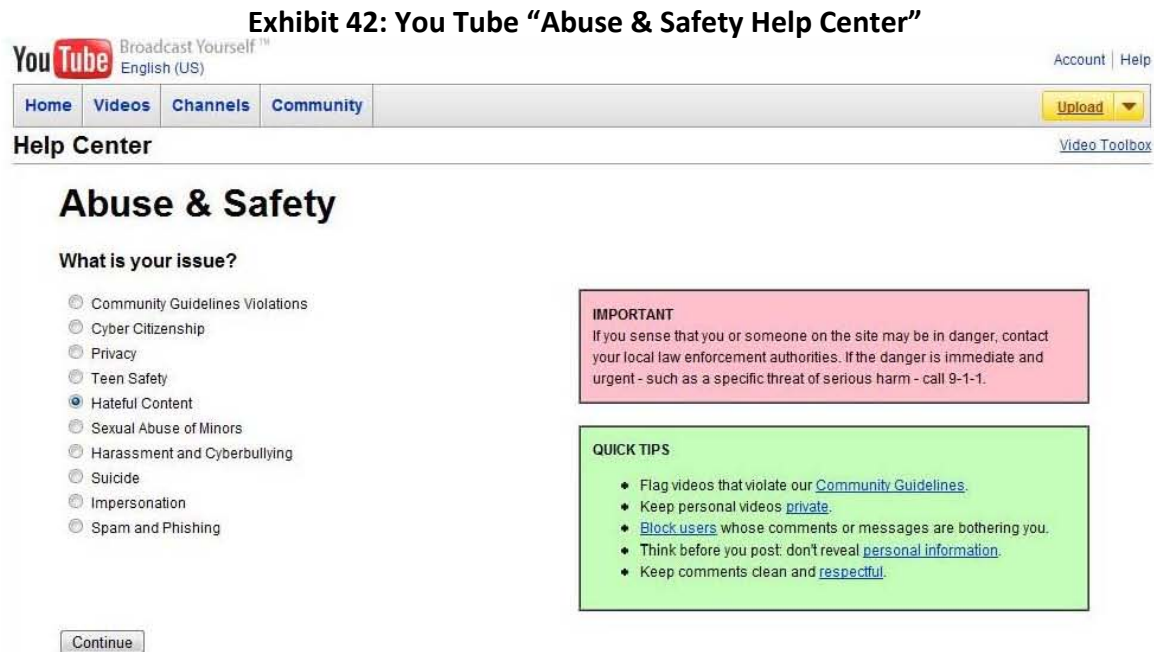
In many instances, MySpace doesn’t create problems, it simply reveals them. Teenagers face difficult decisions and peer pressure nearly every day. Some parents don’t want to admit that their children struggle with sexual temptations, drinking opportunities, drug-related issues, depression, or loneliness. But most teenagers do face most of those pressures. In the past, parents were able to turn a blind eye to these issues and act as if they didn’t exist. But in the virtual world, teens are writing down their problems and reaching out for help. Instead of guessing about our ignoring the issues that teenagers have, we have the unique opportunity through portals such as MySpace to understand their problems and provide help.²⁴²

Many parents are increasingly concerned about the growing problem of cyberbullying. Again, sites are responding to this demand with new tools and reporting features. Sue Shellenbarger of the *Wall Street Journal* notes that “YouTube and some social-networking sites are making it easier to report abuses such as cyberbullying, in which kids—and, appallingly, some adults—use online postings and emails to hurt others. The trend puts more tools in the hands of parents whose kids are the targets or the perpetrators of bullying.”²⁴³ Moreover, when children place cyberbullying videos online, it gives school administrators, law

²⁴² Jason Illian, *MySpace, MyKids* (Eugene, OR: Harvest House Publishers, 2007), p. 13.

²⁴³ Sue Shellenbarger, “Cyberbully Alert: Web Sites Make It Easier to Flag Trouble,” *Wall Street Journal*, December 16, 2008, http://online.wsj.com/article_email/SB122947489283812469-1MyQjAxMDI4MjE5NzQxNzc0Wj.html

enforcement authorities, and others the chance to review the incident, track down the parties involved, and intervene as is appropriate.²⁴⁴



In late 2008, YouTube created a new “Abuse and Safety Center” to make it easier for users to report abusive behavior or inappropriate content.²⁴⁵ The site makes it easy for users to find helpful information from various expert organizations who deal with troubling behavior. For example, if a YouTube user reports “hateful content,” they are directed to tips from the Anti-Defamation League. Similarly, information from the National Suicide Prevention Lifeline is provided to those who report suicide concerns, and the National Center for Missing & Exploited

²⁴⁴ For example, following a skirmish at Beaufort High School in South Carolina that was captured on video and uploaded to YouTube, Beaufort Police Chief Matt Clancy told his local paper that a video of a fight or any other crime posted online makes the job of investigators easier when identifying possible suspects. “It’s a great tool for us,” he told the *Beaufort Gazette*. “You’ve got it on video, and you can identify the person and see what they’re doing.” See Patrick Donohue, YouTube Gives Beaufort High Skirmish Wide Exposure,” *Beaufort Gazette.com*, April 2, 2009, www.islandpacket.com/1482/story/802554.html

²⁴⁵ “Safety, Education, and Empowerment on YouTube,” *Google Public Policy Blog*, December 11, 2008, <http://googlepublicpolicy.blogspot.com/2008/12/safety-education-and-empowerment-on.html>

Children provides information and links about sexual abuse of minors. YouTube also has strict “community guidelines” governing appropriate behavior on the video-sharing site.²⁴⁶

6. The Importance of Website Labeling, Metadata Tagging, and Community Policing

Many of the parental control tools mentioned throughout this filing rely on labeling schemes and metadata tagging. As explained in previous sections, metadata are machine-readable digital data that describe audiovisual media content. For example, MPAA movie ratings and ESRB video game ratings are digitally embedded within DVDs and video games so that other parental control tools (*e.g.*, DVD players, computers, video game consoles) can be used to screen out unwanted content.

This same approach can work for Internet websites. Machine-readable content descriptors can be embedded within websites or online content to “tag” the sites, pages or specific content. Once tagged, such material can be automatically screened by other devices (*e.g.*, filters, operating systems) regardless of how that material is accessed.

The Internet Content Rating Association (ICRA),²⁴⁷ which is part of the Family Online Safety Institute (FOSI),²⁴⁸ is helping to develop improved Internet filtering systems through comprehensive website labeling and metadata tagging. ICRA has created a wide variety of content descriptors that website operators can use to self-label their sites. ICRA does not rate

²⁴⁶ “YouTube Community Guidelines,” www.youtube.com/t/community_guidelines

²⁴⁷ www.fosi.org/icra

²⁴⁸ www.fosi.org

Internet websites or the content itself, leaving it to the content providers to do so using the ICRA labeling system.²⁴⁹ ICRA's website provides additional detail about how the system works:

The centerpiece of the organization is the descriptive vocabulary, often referred to as "the ICRA questionnaire." Content providers check which of the elements in the questionnaire are present or absent from their websites. This then generates a small file containing the labels that is then linked to the content on one or more domains....

The descriptive vocabulary was drawn up by an international panel and designed to be as neutral and objective as possible. It was revised in 2005 to enable easier application to a wide range of digital content, not just websites. Most of the items in the questionnaire allow the content provider to declare simply that a particular type of content is present or absent. The subjective decision about whether to allow access to that content is then made by the parent.²⁵⁰

Once these metadata labels have been embedded within websites, parents can freely download the "ICRAplus" filter from ICRA's website and customize it to their specific needs / tastes.²⁵¹ Or they can use unaffiliated filters or computer operating system controls to screen content by ICRA labels.

Other metadata labeling initiatives exist. The Association of Sites Advocating Child Protection (ASACP), a nonprofit organization founded in 1996 by the adult entertainment industry to eliminate child pornography from the Internet.²⁵² ASACP also works to help parents prevent children from viewing age-inappropriate material online through its "Restricted to Adults" (RTA) website metadata labeling initiative.²⁵³ The RTA label is a general descriptor that all adult entertainment website operators are encouraged to use to help parents who wish to

²⁴⁹ For a description of the ICRA labels and the labeling process, see www.icra.org/label/generator

²⁵⁰ See "About ICRA," www.fosi.org/icra

²⁵¹ www.icra.org/icraplus

²⁵² www.asacp.org

²⁵³ www.rtalabel.org

block all such content. Incidentally, websites using the RTA metadata tag can use it in conjunction with more descriptive ICRA metadata labels.

Microsoft also has an “Essential Metadata Initiative” that works in conjunction with a wide variety of organizations to develop digital metadata tags for media content.²⁵⁴ Specifically, Microsoft works closely with the Geneva, Switzerland-based International Standard Audiovisual Number International Agency (ISAN-IA), which operates the International Standard Audiovisual Number (ISAN). ISAN is a widely recognized, global content labeling system for digital audiovisual material.²⁵⁵

Although generally known for helping content creators manage their intellectual property rights, ISAN tags can also be useful in identifying many other attributes of the underlying content. Specifically, content rating and labeling information can be embedded within the ISAN tag. Microsoft products such as Vista and Internet Explorer can read ISAN metadata tags and filter accordingly.²⁵⁶ Also, the motion picture industry is using ISAN tags to better identify its content, and rating information from various countries is included in those tags.²⁵⁷ According to Patrick Attallah, ISAN Managing Director, as of April 2007, the ISAN

²⁵⁴ “International Organization Licenses Microsoft’s New Multicolor Bar Code Technology for Identifying Audiovisual Works,” Microsoft Corporation, *Press Release*, April 16, 2007, www.microsoft.com/Presspass/press/2007/apr07/04-16MSBarCodePR.mspx

²⁵⁵ www.isan.org

²⁵⁶ Kevin J. Comerford and Michael A. Dolan, “ISAN Implementation in Windows Media Technologies,” Microsoft Corporation, May 2006, www.isan.org/docs/ISAN%20Implementation%20in%20WindowsMedia%20May%202006.pdf

²⁵⁷ “Audiovisual Works Identification for the Motion Picture Studio: Conceptual, Operational, and Technical,” Motion Picture Association of America, 2007.

identification and metadata system supported over 90 different content-specific tags and more than 50 worldwide rating systems in over 35 languages.²⁵⁸

Metadata tagging can also be done by average users for a great deal of user-generated content.²⁵⁹ On popular websites like YouTube, Flickr, MySpace, and others, individuals can label much of their content with various descriptors. These and other sites also allow readers or viewers to tag the content created or posted by others. Most sites also allow users to flag inappropriate or content or abusive communications. Website operators can then deal with the offending content or individuals.

IV. THE PERILS OF MANDATORY CONTROLS, RESTRICTIVE DEFAULTS OR “UNIVERSAL” RATINGS

It is apparent from the language of the Child Safe Viewing Act²⁶⁰ as well as the Commission’s *Notice*²⁶¹ that Congress and the Commission are both interested in finding more “universal” solutions to parental control concerns. This is entirely understandable.

Ultimately, however, the search for technological silver-bullet solutions and “universal” ratings or controls represents a quixotic, Holy Grail-like quest. Simply stated, if it sounds too good to be true, it probably is. There are no simple solutions or quick fixes to concerns about

²⁵⁸ E-mail conversation on April 17, 2007, on record with author.

²⁵⁹ Dan Farber, “The Next Big Thing: User-Contributed Metadata,” *ZD Net.com*, October 29, 2007, <http://blogs.zdnet.com/BTL/?p=6779&tag=nl.e550>

²⁶⁰ Section 2(a) of the Child Safe Viewing Act says the FCC shall examine “the existence and availability of advanced blocking technologies that are compatible with various communications devices or platforms” and Section 2(b) says the Commission shall consider blocking technologies that “may be appropriate across a wide variety of distribution platforms, including wired, wireless, and Internet platforms.”

²⁶¹ Commenting on the language from Section 2(a) and 2(b) of the Child Safe Viewing Act, the Commission argues that, “This language makes it clear that we are to consider blocking technologies appropriate for use on a variety of devices that transmit audio and video programming.” FCC, Child Safe Viewing Act Notice at ¶7.

objectionable media content or online child safety. Only a “layered” approach—involving many tools, methods, and strategies—can get the job done right. And technological blocking controls are probably the *least* important part of that mix. Education and mentoring are far more important.

Moreover, for the reasons stated below, any move to force “universal,” top-down solutions could destroy future innovation in this space. This section will discuss the unforeseen downsides to mandating controls and defaults as well as efforts to create universal rating or labeling schemes.

A. Why Mandatory Controls or Defaults Will Backfire

During ongoing debates about parental controls, ratings, and online child safety, there have occasionally been rumblings about the possibility of requiring that media, computing and communications devices: (1) be shipped to market with parental controls embedded, and possibly, (2) those controls being defaulted to their most restrictive position, forcing users to opt-out of the controls later if they wanted to consume media rated above a certain threshold.

Imagine, for example, a law requiring that every television, TV set-top box, and video game console be shipped with on-board screening technologies that were set to block any content rated above the most general ratings (“G” for movies, “TV-Y” for television, or “E” for video games); this requirement would constitute the most restrictive default for each type of media. Similarly, all personal computers or portable media devices sold to the public could be required to have filters embedded that were set to block all “objectionable” content, however defined.

If “default” requirements such as this were mandated by law, parents would be forced to opt-out of the restrictions by granting their children selective permission to media content or

online services. In theory, this might help limit underage access to objectionable media or online content. Such a mandate might be viewed as less intrusive than direct government censorship and, therefore, less likely to run afoul of the Constitution. For these reasons, such a proposal would likely have great appeal to some policymakers, family groups, child safety advocates, and parents. But mandating parental controls and restrictive defaults is a dangerous and elitist idea that must be rejected because it will have many negative unintended consequences without being likely to achieve the goal of better protecting our kids.

1. You Can Lead a Horse to Water, But You Can't Make It Drink

One of the enduring mysteries about parental controls is why many parents do *not* take advantage of the tools and options at their disposal. It's the proverbial "you can lead a horse to water, but you can't make it drink" problem. There are a few reasons why this may be the case.

As discussed in Section VI, many households may not take advantage of parental control tools because they instead rely on a variety of non-technical "household media rules." Moreover, as shown in Section II, technical controls and rating systems are viewed as unnecessary in many homes where kids are below or above a certain age. Many parents of children under 4 or 5 years of age, for example, do not let their kids consume much media, or they at least exercise much tighter control over their children's media consumption habits. And after kids reach their mid-teen years, many parents eschew technical controls because they either trust their kids, or better yet, they constantly talk to them about media content and their online experiences.

Of course, it could also be the case that some parents do not use technical controls or rating systems because they find them too confusing. That may be true to some extent, but it is important to note that these controls and rating systems are becoming increasingly easy to use.

Most parental control tools are just one or two clicks away on most TVs, gaming systems, or personal computers. And although there are different rating schemes for different forms of media, those rating systems share much in common and are all quite descriptive. Setting up parental controls is certainly no more difficult now than programming a personal video recorder or uploading digital photographs to the Internet.

Finally, it may be the case that some parents are simply not aware of the controls or ratings. This too, however, is increasingly unlikely. Survey data suggests a growing familiarity with most rating systems (some more than others). Companies and non-profit organizations are increasingly offering more information and tutorials along with the parental control tools that are typically embedded, free-of-charge, in almost all modern media devices. In any event, the answer to concerns about insufficient parental awareness is not imposing restrictive mandatory defaults but, as I explain below, increased educational efforts.

Still, for whatever reason, many parents are not using parental controls or rating systems and, at the same time, many feel or express some concerns about being able to manage media use by their children. Regardless of the culprit—and it could be a combination of all of the factors listed above—what more could be done to encourage these parents to use existing technical controls and rating systems to limit children’s access to potentially objectionable content or communications? There are two general options.

One way to increase parental comfort levels is through better education and awareness-building initiatives. Many companies already offer detailed information and tutorials along with the parental control tools they offer, but more could always be done to promote awareness of the tools and how to use them. Many parents may feel they cannot effectively manage media

use in their homes because they are unaware of their options or unsure how to utilize the available tools.

One sensible first step is the inclusion of easy-to-understand instructions in all user manuals. “Tip sheets” could also be bundled along with the products, which provide a summary of how set up parental controls, or what relevant ratings meant. Most vendors already offer this and much more on their websites, but sometimes the links to those pages can be difficult to find. All media companies should consider placing clearly labeled links on their websites to guide visitors to parental controls, ratings information, or online safety tips. Finally, customer support hotlines—whether automated and human-based—could probably be improved and expanded.

Again, most companies are already moving in this direction today. It’s simply a smart business practice since many parents increasingly expect such services to be available. To the extent some companies aren’t keeping up, others—policymakers and child safety groups, in particular—are increasing putting pressure on them to provide such tools and assistance.

The second approach to encouraging more widespread use of parental controls and rating systems would involve the sort of legal mandates described above. Presumably, this would require a law or regulation that would: (1) spell out what sort of controls or filters would be embedded in every “media or computing device” and then, (2) determine how restrictive the default control settings would be before the hardware or software in question was marketed. In essence, this would be a mandatory “opt-out” regime for parental controls/filters.

The first portion of the mandate is largely unnecessary, as almost all major media devices marketed today already contain some kind of parental controls: All TVs include V-chips, all set-top boxes include additional TV screening controls, and all video game consoles include

blocking tools for both games and movies. With PCs, filters and monitoring tools have been made ubiquitously available by ISPs and non-profits for little or no charge, and newer operating systems such as Windows Vista include powerful parental control tools. Importantly, almost all of these tools are free-of-charge. A variety of supplementary tools can be purchased online or from electronics retailers or computer stores. As a general matter, moreover, it is rarely sound public policy to have governments—rather than markets—select a particular technology or service as a mandatory feature. This risks locking in less effective technologies and perhaps also creating financial windfalls for well-connected vendors of such technologies.

The real debate, then, comes down to the question of how effective those embedded controls are at meeting the interests of parents, and whether the embedded controls should have pre-established defaults set to the most restrictive setting available before they are shipped or downloaded. Of course, any company could *voluntarily* offer such an alternative today. It's worth asking, therefore, why are no companies currently doing so?

2. Enforcement Hassles

There are many reasons why no media or communications companies are currently offering such maximally restrictive defaults when they ship their products to market. Those reasons are instructive when considering the wisdom of mandating that such defaulted controls be mandated by law.

To begin, there's just not as much demand for this as some might think. Again, not all homes have children in them. And, in those that do, not all those parents see the need to use parental controls or ratings, usually because they rely on household rules or tightly monitor or restrict access to media and communications devices.

Moreover, because there are many adults who purchase media devices for their own use, it would be illogical to ship *all* devices or products to market with the controls set to the most restrictive setting.²⁶² In fact, many consumers (even some who are parents themselves) would likely find it annoying, and perhaps even somewhat insulting, to be forced to opt-out of such controls when they purchase new media hardware or software. And it's likely that as soon as such devices or services hit the market, consumer complaint hotlines would light up like Christmas trees due to calls from irate users griping about what they imagine to be defective hardware or software.

Could companies offer multiple versions of their hardware or software products to solve this problem? For example, some set-top boxes, gaming consoles, and PCs could be sold and labeled as “Kid-Friendly” (or “locked”) while others are “Adult-Only” (or “unlocked”). It goes without saying that this would represent a major expense to many vendors (especially hardware vendors). It could also create potential confusion when the devices are labeled and marketed for sale. And what would the penalty be for a mislabeled device, or the accidental sale of such a device to a minor?

3. Perverse Incentives and Possible Evasion

It may be that there is a market for such “kid-friendly” devices or services. There are, for example, some wireless device and service options designed for kids that have limited features, or some toy (and toy-like) devices that have filters on by default, or only work with certain age-appropriate internet services. Many social networking services designed for kids

²⁶² This is true even for video game consoles. For example, according to a survey by Hart Research, the average age of a video game purchaser is 40. See: *Essential Facts about the Computer and Video Game Industry: 2006 Sales, Demographics and Usage Data*, Entertainment Software Association, 2005, p. 3, www.theesa.com/archives/files/Essential%20Facts%202006.pdf

have strict settings on by default. These may well be fantastic choices for some parents and kids. But whether that is the case seems to be best determined by the market.

Particularly for mass-market general use devices like PCs and televisions, mandating the offering of dual versions (“locked”/“kid-friendly” and “unlocked”) seems likely to create perverse incentives, both for consumers and for media and technology providers. If services and devices are sold with the highest levels of restrictions active by default, many parents might seek to avoid the annoyance associated with the “kid-friendly” versions of the device and just purchase “unlocked” hardware or software. And kids would likely get quickly to work cracking the defaults on the kid-friendly versions of the hardware or software.²⁶³ The result would be some significant degree of consumer dissatisfaction with restrictive-default services and, except perhaps in the case of households with very young children, dissatisfaction with locked/kid-friendly services and devices.

Among the possible consequences of such a dual version mandate would be a perverse incentive for service providers and device makers to avoid investing in parental control tools. If setting controls to the highest default level is mandatory, but at the same time most consumers don’t prefer that default level, some consumer backlash is inevitable. And when consumers are unhappy about a service feature—but companies are not permitted to address that unhappiness by turning off the higher settings—a likely result could be for companies to weaken or even not offer parental controls altogether.

²⁶³ Witness what happened in Australia within a few days of the government releasing subsidized filtering software. A 16-year old Melbourne schoolboy cracked the Australian government’s \$84 million internet porn filter in just over 30 minutes. See Nick Higginbottom and Ben Packham, “Student Cracks Government’s \$84m Porn Filter,” *News.com.au*, August 26, 2007, www.news.com.au/story/0,23599,22304224-2,00.html

There are other problems involved in enforcing such a mandate. Regulators would need to grapple with the possibility of widespread evasion in terms of offshore sales and black market devices. For example, would it be illegal for an eBay vendor located in Hong Kong to sell a U.S.-based customer an “unlocked” PlayStation Portable without first verifying that they are indeed an adult? If so, that’s another layer of regulation that needs to be considered in terms of online age verification.²⁶⁴

Of course, governments could forbid the development of “unlocked” devices or software and mandate that every media or computing device sent to market had defaults set to maximum restrictiveness. Even assuming such rules would not run afoul of international trade law, many of the same problems would still develop, however. It would likely be difficult to stem the flow of illegal devices or software, and hackers would likely only work harder to defeat existing controls. And what about all the existing “unlocked” devices already on the market? This mandate might breathe new life into older devices and discourage some consumers from making the jump to new hardware and software that includes superior parental control tools.

A final enforcement question relates to how broadly “media devices” are defined for purposes of this mandate. TVs, set-top boxes, gaming consoles and PCs would all be covered, of course. But what about mobile phones, iPods, MP3 players, PlayStation Portables and GameBoys, and so on? If “media devices” is defined broadly enough, it would bring an unprecedented array of consumer electronic devices and communications technologies under the purview of the FCC. Each class of devices would likely have its own set of enterprising

²⁶⁴ Adam Thierer, “Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,” Progress & Freedom Foundation *Progress on Point* No. 14.5, March 21, 2007, www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf

hackers and renegade device makers, eager to evade the mandates. Presumably, financial penalties would be required and various enforcement actions would be sanctioned in an attempt to thwart such activity. Finally, as a result of these new mandates, the prices of all the affected media devices would likely rise for consumers.

4. Unintended Consequences and Constitutional Concerns

A proponent of mandatory defaults might object that regulation is often difficult, even expensive, but we still find ways to enforce many other laws—if only to try to teach the public, or kids, a lesson. In this case, some slippage in the system might be viewed as an acceptable trade-off for increased awareness among some parents about parental control tools or potentially objectionable media content or forms of online communications.

But this mentality myopically ignores the many unintended consequences of such a regulatory regime. The fundamental problem with a mandate of this sort is that, while well-intentioned, *it threatens to upset the current balance of things and could leave parents and their children less well off.*

As explained above, there has never been a time in our nation’s history when parents have had more tools and methods at their disposal for controlling their children’s media consumption. Indeed, on the whole, parents are gaining control, not losing it, with technological innovation. It would be foolish, however, to think that this trend might not be slowed, or even reversed, by misguided public policy prescriptions. One of the most unfortunate consequences of mandatory defaults would be lulling some parents into a false sense of security: If parents came to believe that, because a filter was installed, they need do nothing more to help their children go online safely, or to remain engaged in their children’s media consumption, that would be an extremely troubling outcome.

Moreover, as was noted above, a rule mandating restrictive parental control defaults might create perverse incentives for industry to *not* rate content or build better controls at all. After all, it is important to remember that the ratings and controls that government is seeking to regulate here are *voluntary and private*; there is no reason they couldn't be abandoned tomorrow. Of course, if they were abandoned that might lead to calls for government intervention or regulation and the substitution of some sort of universal ratings regime for the voluntary systems that exist today. If that occurred, lawmakers would be likely pressured into either making content-based determinations or mandating that a private organization do the same thing; either response would likely run afoul of the First Amendment.

But even if voluntary rating systems remained in place as the basis of a new federal enforcement regime, there *are* some constitutional issues in play here. Namely, it would be unconstitutional for government to enshrine a private ratings scheme into law or use it as a trigger for legal liability. That is what several courts have held in past years after some state and local governments attempted to enact laws or ordinances based upon the MPAA's voluntary movie ratings system.

For example, in *Borger v. Bisciglia* a U.S. District Court held that "[A] private organization's ratings system cannot be used to determine whether a movie receives constitutional protection."²⁶⁵ Similarly, in *Swope v. Lubbers*, the court held that "[t]he standards by which the movie industry rates its films do not correspond to the... criteria for determining whether an item merits constitutional protection or not."²⁶⁶ Roughly a dozen court cases have come to largely the same conclusion: Government cannot co-opt a voluntary, private ratings

²⁶⁵ *Borger v. Bisciglia*, 888 F. Supp. 97, 100 (E.D. Wis. 1995).

²⁶⁶ *Swope v. Lubbers*, 560 F. Supp. 1328, 1334 (W.D. Mich. 1983).

system for its own ends.²⁶⁷ Recent video game cases have reached similar conclusions.²⁶⁸ Thus, a law mandating parental control defaults based on voluntary ratings systems will likely end up in court and become the subject of another protracted legal battle between government and industry.

5. Are Mandatory Default Really Necessary?

Finally, it's worth noting that most media, communications, and computing devices cost substantial sums of money. Televisions, movies, video games, cell phones, MP3 players, computers, and so on, do not just drop from high-tech heaven into our kids' laps! When our kids want those things—or want things that are advertised on those media platforms—they must come to parents and ask for money (usually a lot of it). As Section VIII notes, this “power of the purse” is, in many ways, the ultimate parental control tool. If parents are shelling out money for such devices, they are presumably also in a good position to set some rules about the use of those devices once they are brought into the home. Whether those rules take the form of informal household media rules (see Section VI) or technical parental controls (see Section III) is, ultimately, a decision that each family must make for themselves. There is no reason for government to make that decision preemptively for *all* households by mandating highly restrictive parental control defaults.

²⁶⁷ *Interstate Circuit v. Dallas*, 390 U.S. 676 (1968); *Drive in Theaters v. Huskey*, 305 F. Supp. 1232 (W.D.N.C. 1969); *Engdahl v. City of Kenosha*, 317 F. Supp. 1133 (E.D. Wis. 1970); *Motion Picture Association of America v. Specter*, 315 F. Supp. 824 (E.D. Pa. 1970); *State v. Watkins*, 191 S.E. 2d 135 (S.C. 1972); *Watkins v. South Carolina*, 413 U.S. 905 (1973); *Potter v. State*, 509 P.2d 933, (Okla. Ct. Crim. App. 1973); *Neiderhiser v. Borough of Berwick*, 840 F.2d 213 (3d Cir. 1988); *Gascoe, Ltd. v. Newtown Township*, 699 F. Supp. 1092 (E.D. Pa. 1988).

²⁶⁸ Adam Thierer, “Fact and Fiction in the Debate Over Video Game Regulation,” Progress & Freedom Foundation *Progress on Point* 13.7, March 2006, <http://www.pff.org/issues-pubs/pops/pop13.7videogames.pdf>

Moreover, there are better ways for government and industry to encourage the diffusion and adoption of parental control tools and rating systems. Instead of spending money litigating cases against the government, industry should plow their resources into improved, easier-to-use parental control tools and consumer education efforts. And government education and awareness-building campaigns could go a long way toward improving consumer adoption. In the past, government has helped change public attitudes about safety in other contexts by undertaking (or lending support to) various public awareness campaigns, including: forest fire prevention efforts (“Smokey the Bear” campaigns); anti-littering efforts (“Give a Hoot, Don’t Pollute”), and seat-belt safety. Those campaigns have helped forever change behavior and improved public safety as a result.

Policymakers should tap these more constructive, constitutional solutions and steer clear of mandating parental controls and restrictive default settings that would, ultimately, have many unintended consequences and leave parents and children worse off in the long run.

B. Why Mandating Universal Ratings Would Be a Mistake

So-called “universal ratings” schemes would suffer from many of the same problems that would plague mandatory parental controls or defaults.

1. We Already Have Universal *Sectoral* Ratings

First, however, it is important to acknowledge the fact that while we do not have a “universal rating” system across all media—television, movies, music, video games, and the Internet—the current voluntary rating systems *are* universal, or nearly universal, within their respective sectors.

The same cannot be said of current “independent” ratings schemes. Although those systems provide parents with beneficial information, they fall well short of being as

comprehensive as official industry-based rating systems. For example, Common Sense Media provides the public with a wonderful informational resource that freely offers detailed reviews of new movies, television programs, video games, music, and more.²⁶⁹ Still, Common Sense Media does not come anywhere close to rating all the media content emanating from those sectors. More obscure titles typically go unrated by the organization, and older content that pre-dates the organization remains largely unrated. Moreover, there is no guarantee that independent rating sites will exist forever. Indeed, many independent media review sites and services have come and gone over the past decade.

Finally, official industry rating systems establish a sort of baseline for all other rating systems. Not only does the public—and parents in particular—use the official rating systems as a rough proxy for whether or not content is acceptable for their kids, but independent rating services also use the official industry ratings as point of comparison. As Section VII notes, this represents a healthy form of competition among official rating systems and independent systems, with the independent groups providing a useful “watchdog” role in this regard. The public is better off for having access to *both* industry and independent rating schemes.

2. Mandating Universe Ratings Would Destroy Innovation and Impose Serious Costs on Media Providers and Consumer Electronics Companies

Mandating “universal” controls and ratings across all media platforms could destroy innovation in this space by substituting a government-approved, “one-size-fits-all” standard for today’s “let-a-thousand-flowers-bloom” approach, which offers diverse tools for a diverse citizenry.

²⁶⁹

www.common sense media.org

At a minimum, a universal ratings mandate would erase years' worth of educational efforts by industry and others to inform the public about existing rating systems. Crafting a new ratings scheme for all media would require a massive public re-education effort that would create confusion in the interim with no guarantee of success in the long-run.

A universal rating mandate or mandatory technological “silver-bullet” solution would also impose significant costs on media providers and consumer electronics (CE) companies. Complying with such a mandate would force media creators to re-train the employees who label new content, re-label their back catalogs of content, and re-educate their consumers about the new system. For manufacturers of CE and digital media devices, the costs associated with a universal ratings mandate would also be steep. Each new device capable of receiving media content that was required to be rated and filterable would have to be equipped with new filtering technology. Moreover, all legacy content and devices would become a casualty of regulation: Because it is unlikely they could be made backwards-compatible, they would suddenly become obsolete-by-regulation—at a significant economic loss to manufacturers and vendors who would be pressured to dispose of their inventory.

3. “Scientific Ratings” Are a Fiction

As noted in Section I, media rating and content-labeling efforts are not an exact science but a fundamentally subjective exercise. While some academics have suggested that ratings can be made more “scientific,” the reality is that rating and labeling artistic expression will always be highly contentious. Attempting to give a rating system the aura of “science” implies that the process would be more authoritative or trustworthy, but there is no evidence to show why that would be the case. Indeed, even medical sciences can be tainted by social and political prejudices. As Oliver Wendell Homes, Sr. wrote in 1860:

The truth is, that medicine, professedly founded on observation, is as sensitive to outside influences, political, religious, philosophical, imaginative, as is the barometer to the changes of atmospheric density. Theoretically it ought to go on its own straightforward inductive path, without regard to changes of government or to fluctuations of public opinion. But look a moment while I clash a few facts together, and see if some sparks do not reveal by their light a closer relation between the Medical Sciences and the conditions of Society and the general thought of the time, than would at first be suspected.²⁷⁰

This is not to say all medical practitioners who might favor universal rating schemes would always be tainted by social forces or political considerations. But if responsibility for the creation and administration of any universal ratings scheme was left to the “medical community,” one wonders what would stop other groups or forces that *did* have a political agenda from coming to have more of a say in the rating process. Again, this raises the “heckler’s veto” problem since a vocal minority’s preferences could trump those of the public at large.²⁷¹

Practically speaking, the problem with this approach is that it raises the prospect of gridlock and delay in getting content rated and made available to consumers on a timely basis. If every movie, television program, album, video game, and so on, were required to be rated by some sort of “blue-ribbon” task force made up of academic experts, media “experts,” child psychologists, and so on, how long would it take to get their approval? Would the panel have the right to prohibit some media content from being released altogether? Would they have the power to fine retailers for non-compliance with their new system?

²⁷⁰ Oliver Wendell Holmes, Sr., “Currents And Counter-Currents In Medical Science,” *Medical Essays: 1842-1882* (Boston: Houghton Mifflin Company, 1861), <http://books.google.com/books?id=TsgNAAAAYAAJ&output=html>

²⁷¹ *Reno v. ACLU*, 521 U.S. 844, 880 (1997).

Of course, there is nothing stopping anyone, including medical organizations, from voluntarily bringing together a group of independent experts to create alternative guidelines or independent rating systems. But having such systems enshrined by law raises many thorny Constitutional and practical questions.

4. Mandatory Universal Ratings Would Raise Profound First Amendment Concerns

The notion that the government should have a say in how speech and artistic expression is rated and labeled raises serious First Amendment issues.²⁷² As noted above, many courts have held that it would be unconstitutional for government to enshrine any private ratings scheme into law or use such a scheme as a trigger for legal liability. A mandatory universal rating scheme would raise even more profound First Amendment concerns since it tiptoes dangerously close to the definition of prior restraint and/or compelled speech.

Presumably, if government required all content to be labeled according to some “universal” standard or scheme, it would require that the government have some say in creating, or at least blessing, that standard and then stipulating penalties for non-compliance with that rating scheme. This is where a subtle—if not explicit—form of prior restraint would enter the picture.

As the Supreme Court stated in *Bantam Books Inc. v. Sullivan* (1963), “Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity.”²⁷³ In that case, the Court struck down as unconstitutional a Rhode Island measure which had created a Commission “to educate the public concerning any book...

²⁷² My thanks to my PFF colleague Berin Szoka for his assistance in constructing this section.

²⁷³ *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963).

or other thing containing obscene, indecent or impure language, or manifestly tending to the corruption of the youth as defined [in other sections] and to investigate and recommend the prosecution of all violations of said sections.” The Court found that the Rhode Island Commission to Encourage Morality in Youth had engaged in “informal censorship” when it:

notif[ied] a distributor that certain books or magazines distributed by him had been reviewed by the Commission and had been declared by a majority of its members to be objectionable for sale, distribution or display to youths under 18 years of age. Such notices requested the distributor's "cooperation" and advised him that copies of the lists of "objectionable" publications were circulated to local police departments and that it was the Commission's duty to recommend prosecution of purveyors of obscenity.²⁷⁴

Similarly, in *Interstate Circuit v. Dallas* (1968), the Supreme Court struck down as unconstitutionally vague an ordinance authorizing the classification of certain films as “not suitable for young persons” where the standard was defined as “describing or portraying brutality, criminal violence or depravity in such a manner as to ... incite or encourage crime or delinquency on the part of young persons.”²⁷⁵ In *Interstate Circuit*, the Court also noted that “there has been no retreat in this area from rigorous insistence upon procedural safeguards and judicial superintendence of the censor's action” and cited a long string of cases in support of that notion.²⁷⁶ Since that time, the Supreme Court and lower courts have continued to strike down all prior restraint laws and state and local ordinances dealing with content labeling requirements.

²⁷⁴ *Id.* at 58.

²⁷⁵ *Interstate Circuit, Inc. v. City of Dallas*, 390 U.S. 676 (1968).

²⁷⁶ *Id.* at 682-3. The other decisions cited by the court were: *Freedman v. Maryland*, 380 U.S. 51 (1965); *Winters v. New York*, 333 U.S. 507 (1948); *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495 (1952); *Gelling v. Texas*, 343 U.S. 960 (1952); *Superior Films, Inc. v. Department of Education*, 346 U.S. 587 (1954); *Commercial Pictures Corp. v. Regents*, 346 U.S. 587 (1954); *Holmby Productions, Inc. v. Vaughn*, 350 U.S. 870 (1955).

More recently, in a series of video game-related cases, Federal appellate and district courts have consistently struck all state and local efforts aimed at imposing labels on video games or co-opting the video game industry's rating system and giving it the force of law. In two of the most recent of these cases, appellate courts struck down similar state laws banning the sale of certain video games to minors and mandating that retailers place a label with the numerals "18" on such games.²⁷⁷

The two circuit courts agreed that the labeling mandates constituted compelled speech—namely, the state's conclusion that a particular video game was inappropriate for minors because it qualified as "sexually explicit" (Illinois) or "violent" (California). Both courts agreed that the government could compel only the disclosure of "purely factual and uncontroversial information" for the sake of consumer protection, such as product warning labels about mercury content or, in an attorney's advertisement, the fact that clients might be responsible for costs of litigation.²⁷⁸ By contrast, the Seventh Circuit concluded that Illinois's label "communicates a subjective and highly controversial message—that the game's content is sexually explicit," a message that the court declared "non-factual," "far more opinion-based than the question of whether a particular chemical is within any given product," and "unlike a surgeon general's warning of the carcinogenic properties of cigarettes."²⁷⁹ The Ninth Circuit reached the same conclusion and, while declining to adopt the Seventh Circuit's application of

²⁷⁷ *Video Software Dealers Association v. Arnold Schwarzenegger*, 556 F.3d 950 (9th Cir. 2009) (*Schwarzenegger*); *Entertainment Software Association v. Blagojevich*, 469 F.3d 641 (7th Cir. 2006) (*Blagojevich*).

²⁷⁸ See *Blagojevich*, 469 F.3d at 651-52 (citing *Nat'l Elec. Mfrs. Ass'n v. Sorrell*, 272 F.3d 104, 114-16 (2d Cir. 2001); *Zauderer v. Office of Disciplinary Counsel for Sup. Ct. of Ohio*, 471 U.S. 626, 651 (1985)); see *Schwarzenegger*, 556 F.3d at 966-67.

²⁷⁹ *Blagojevich*, 469 F.3d at 652.

the exacting standard of strict scrutiny, concluded that California’s labeling mandate could not survive even the less demanding standard of intermediate scrutiny, also noting that the mandate did not serve to protect consumers against deception.²⁸⁰

These two cases, and the Supreme Court cases on which they rest, make it clear that any universal ratings system compelling disclosure of anything other than “purely factual and uncontroversial information” about content for the sake of preventing deception of consumers would almost certainly be struck down by the courts. Crafting a universal content rating system within these constitutional constraints would be highly challenging and, even if it could be done, the result would be highly unlikely to satisfy those who advocate labeling mandates.²⁸¹

Finally, because the vast majority of content regulated under a mandatory universal rating system would be non-obscene, the constitutional bar would be even higher.

5. Universal Ratings May Evolve Naturally from Increased Metadata Tagging and Crowdsourcing Efforts

The growth of user-generated content and interactive social networking sites and services raises profound challenges for traditional rating systems and government regulation alike. The sheer volume of speech and expression being produced in modern times simply dwarfs all the content created over the past century.

²⁸⁰ *Schwarzenegger*, 556 F.3d at 967 (citing *Zauderer*, 471 U.S. at 651 (requiring that the “disclosure requirements [be] reasonably related to the State’s interest in preventing deception of customers”).

²⁸¹ Of course, to be truly “universal,” a content ratings system would have to apply not only to “professional” content (like existing industry ratings systems), but also to user generated content. But the prior restraint of requiring users to label (or have others label) their content would significantly impair speech and content generation by users who wish to remain anonymous. Noting an honorable tradition of advocacy and of dissent in America and recognizing anonymity as “a shield from the tyranny of the majority,” the Supreme Court has rejected laws that burden anonymous speech, such as prohibitions on anonymous pamphleteering and online age verification mandates for sexually explicit content. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 at 357 (1995). Thus, the hope of a “universal” ratings system appears to be ultimately inconsistent with the First Amendment.

Importantly, however, these new means of communications and content creation are also spawning innovative approaches to content labeling through metadata “tagging” as well as content “flagging,” which refers to user efforts to highlight inappropriate or objectionable content or comments.

Consider the “reputational systems” and user-generated reviews already in place on some major websites. An increasingly important part of the content offered by sites such as Amazon.com, Netflix.com, Metacritic.com, and IMDB.com (the Internet Movie Database) is the detailed reviews posted by users of movies, TV programs, and other types of media content. These reviews can help parents screen content for their children. Better yet, some of those sites allow users to find other users with similar tastes and values and track their reviews regularly. Thus, once a parent finds a particular piece of content they deem suitable for their children, these sites make it easy for that parent to find other content that is likely to match their values—thus “crowdsourcing” to other users the inherently subjective task of rating content and allowing parents to follow reviews from users who seem to share their values.

On sites with a great deal of user-generated content, such as YouTube.com and many social networking sites, users can “flag” inappropriate content through various reporting mechanisms. Once enough users in that online community have flagged a certain post or piece of content as inappropriate, the “wisdom of the crowd” will help site administrators identify which content (or users) the online community feels are problematic. Offending content can then be (and frequently is) removed and users who cause problems can be dealt with, or even removed from the site.

Finally, the increased use of digital metadata tagging can facilitate greater user screening. Metadata, which is essentially data about data, can be embedded in almost any

digital media file. It can be used either by the content creator or downstream parties to embed useful information about content ratings, descriptors, warnings, *etc.* As more and more content gets “tagged and flagged”—by both creators or crowds—it will facilitate easier information retrieval and blocking.

V. WHY MANDATORY AGE VERIFICATION WON’T WORK AND WOULD MAKE KIDS LESS SAFE

The Commission inquires whether age verification technologies might be tapped as a method of restricting underage access to online sites or content.²⁸² The Commission should exercise great caution here since mandatory age verification could potentially make kids *less* safe online.²⁸³

Mandatory age verification represents a dangerous solution to concerns about online child safety because it:

- **Won’t Work:** Mandatory age verification will not work as billed. For the reasons detailed below, it will fail miserably and create more problems than it will solve.
- **Will Create a False Sense of Security:** Because it will fail, mandatory age verification will create a false sense of security for parents and kids alike. It will lead them to believe they are entering “safe spaces” simply because someone has said users are “verified.”
- **Is Not a Background Check:** Moreover, even if age verification did work as billed, it is important to realize it is not synonymous with a complete background check. In other words, even if the verification process gets the *age* part of the process right, that tells us little else about the person being verified.

²⁸² FCC, *Child Safe Viewing Act Notice*, ¶ 41.

²⁸³ For a fuller exploration of these issues, see Adam Thierer, “Social Networking and Age Verification: Many Hard Questions; No Easy Solutions,” Progress & Freedom Foundation *Progress on Point* No. 14.5, Mar. 2005; Adam Thierer, *Statement Regarding the Internet Safety Technical Task Force’s Final Report to the Attorneys General*, Jan. 14, 2008, www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf; Nancy Willard, “Why Age and Identity Verification Will Not Work—And is a Really Bad Idea,” Jan. 26, 2009, www.csriu.org/PDFs/digitalidnot.pdf; Jeff Schmidt, “Online Child Safety: A Security Professional’s Take,” *The Guardian*, Spring 2007, www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf.

- **Is a Grave Threat to Privacy:** Mandatory age verification is dangerous because it would require that even more personal information (about kids, no less) be put online at a time when identity theft and privacy violations continue to be major concerns.
- **Will Seriously Misallocate Resources:** Devising and enforcing age verification regulations might also divert valuable time and resources that could be better used to focus on education and awareness-building efforts, especially K-12 online safety and media literacy education. Moreover, it might divert law enforcement energy and resources away from policing serious crimes or more legitimate threats to children.

A. Age Verification Regulation Has Already Been the Subject of a Protracted Legal Battle

As the Commission no doubt recognizes, age verification technologies and mandates have been the subject of intense legal wrangling over the past decade. Congress passed the Child Online Protection Act (COPA) in 1998 in an effort to restrict minors' access to adult-oriented websites. The measure provided an affirmative defense to prosecution if a website operator could show that it had made a good-faith effort to restrict site access by requiring a credit card, adult personal identification number, or some other type of age-verifying certificate or technology.

The legislation was immediately challenged and was twice reviewed by the Supreme Court. The legal wrangling about COPA's constitutionality continued for over a decade. Finally, in March 2007, Judge Lowell Reed Jr., senior judge of the U.S. District Court for the Eastern District of Pennsylvania, issued a permanent injunction against the enforcement of COPA.²⁸⁴ In July 2008, the full Third Circuit Court of Appeals upheld this injunction,²⁸⁵ and then, in January

²⁸⁴ *American Civil Liberties Union v. Gonzales*, 478 F. Supp. 2d 775 (E.D.Pa. 2007) (*ACLU v. Gonzales*), available at www.cdt.org/speech/copa/20070322copa.pdf.

²⁸⁵ *American Civil Liberties Union v. Ashcroft*, 534 F.3d 181 (3d Cir. 2008) (*ACLU III*), www.cdt.org/speech/20080722COPA3rdCircuit.pdf

2009, the Supreme Court rejected the government’s latest request to revive the law, meaning it is likely dead.²⁸⁶

After considering exhaustive evidence about the state of the art in age and identity verification, Judge Reed held that COPA was unconstitutional because it was not “the least restrictive, most effective alternative in achieving the [government’s] compelling interest” and it remains “impermissibly vague and overbroad.”²⁸⁷ Regarding the effectiveness of age verification, Judge Reed held that, “From the weight of the evidence, I find that there is no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor.”²⁸⁸ Specifically, regarding the use of credit cards as an age verification tool, Judge Reed found that, “payment cards cannot be used to verify age because minors under 17 have access to credit cards, debit cards, and reloadable prepaid cards” and... “there are many other ways in which a minor may obtain and use payment cards.”²⁸⁹

²⁸⁶ See Adam Thierer, “Closing the Book on COPA,” Progress & Freedom Foundation, *PFF Blog*, January 21, 2009, http://blog.pff.org/archives/2009/01/closing_the_book.html.

²⁸⁷ *ACLU v. Gonzales* at 778.

²⁸⁸ *Id.* at 800.

²⁸⁹ *Id.* at 801. “The minimum information required by a DVS [data verification services] company to attempt a verification is a first name, last name, street address, and zip code. This minimum information requirement can easily be circumvented by children who generally know the first and last name, street address and zip codes of their parents or another adult. ... I find from the testimony that without a physical delivery of goods and an accompanying visual age verification, neither the [data verification services] nor the Web page operator can know whether an adult or a child provided the information. Attempting to verify age with this information in a consumer-not-present transaction is therefore unreliable.” *Id.* at 802.

B. Blue Ribbon Online Safety Task Forces Agree that Mandatory Age Verification is Not Workable, Will Not Improve Online Child Safety

In a sense, Judge Reed's decision was unsurprising since many other experts had arrived at the same conclusion in previous studies. For example, Congress enacted COPA in 1998, it also established an expert Commission on Online Child Protection to study methods for reducing access by minors to harmful material on the Internet. As part of its final report, the COPA Commission concluded that credit card-based age verification would be completely inappropriate for instant messaging and chat, the precursors of today's social networking technologies. The Commission found: "This system's limitations include the fact that some children have access to credit cards, and it is unclear how this system would apply to sites outside the U.S. It is not effective at blocking access to chat, newsgroups, or instant messaging."²⁹⁰

More recently, at the request of 49 state attorneys general (AGs), a blue ribbon task force assembled in 2008 by state AGs to study online child safety and potential technological responses to those concerns. The Internet Safety Technical Task Force (ISTTF) reached the following conclusions regarding the effectiveness of mandatory age verification as a technological solution:²⁹¹

²⁹⁰ Commission on Online Child Protection, Final Report, October 20, 2000, www.copacommission.org/report/ageverification.shtml. Also see Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet*, (Washington, DC: National Academy Press, 2002), pp. 206-9, 339-49.

²⁹¹ Full disclosure: I was a member of this task force. See Adam Thierer, "Statement Regarding the Internet Safety Technical Task Force's Final Report to the Attorneys General," January 14, 2008, www.pff.org/issues-pubs/other/090114ISTTFthiererclosingstatement.pdf

Age verification and identity authentication technologies are appealing in concept but challenged in terms of effectiveness. Any system that relies on remote verification of information has potential for inaccuracies. For example, on the user side, it is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to extant records. Any system that focuses on third-party in-person verification would require significant political backing and social acceptance. Additionally, any central repository of this type of personal information would raise significant privacy concerns and security issues.²⁹²

In the months leading up to the ISTTF's formation, AGs had stated their belief that age verification might be an effective means of dealing with concerns about online predation on social networking sites (SNS). As a result, after reading the ISTTF's final report, some policymakers may be disappointed that the ISTTF didn't recommend mandatory age verification as solution, or they may feel that the Task Force should have done more to work through the details of age verification as a solution to online safety concerns. But, if the ISTTF had one failing—and this would really be the only one—it was that it did not go far enough in illustrating why mandatory age verification will *not* work and how age verification will actually make kids *less* safe online.

C. Ten Problems with Mandatory Age Verification as a Solution to Online Safety Concerns

Indeed, to the extent some policymakers persist in this pursuit of a technological “Holy Grail,” they must specifically address the following ten problems with age verification mandates, which explain why such mandates will inevitably fail to protect children online.

²⁹² Internet Safety Technical Task Force, “Enhancing Child Safety & Online Technologies,” Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, December 31, 2008, p. 10, <http://cyber.law.harvard.edu/pubrelease/isttf>

1. The Risk Mismatch Problem

The ISTTF's Research Advisory Board found that the primary online safety issue today is peer-on-peer cyber-harassment, not adult predation. Mandatory age verification would do nothing to stop cyberbullying. Indeed, the lack of adult supervision may even exacerbate the problem.

2. The Non-Commercial Speech Problem

Age verification schemes *may* work for *some* commercial websites where transactions require the transfer of funds, goods, or services. Age verification may also work in those contexts (*e.g.*, online dating services) where users *want* to be verified so others know more about them. But most social networking sites (SNS) involve non-commercial transactions and their users do not want to divulge too much personal information. This will significantly complicate AV efforts.

3. The Data Matching/Processing ("Initial Enrollment") Problem

Online age verification efforts will likely break down first at the *initial enrollment* stage.²⁹³ Because little data exists to verify minors, age verification simply won't work for sites where adults and minors coexist, or to keep adults out of "child-only" sites. Unless we want to force every child to carry a mandatory national ID card—which seems like an extreme and potentially dangerous solution—there isn't an effective way of handling the initial authentication process.

²⁹³

I am indebted to Jeff Schmidt for the useful distinction between the initial enrollment and subsequent visit problems with online age verification. See: Jeff Schmidt, "Online Child Safety: A Security Professional's Take," *The Guardian*, Spring 2007, www.jschmidt.org/AgeVerification/Gardian_JSchmidt.pdf

Some have suggested using schools and school records as a second-best alternative to solve the initial enrollment problem. It is certainly true that using schools and school records will make the initial enrollment process for minors somewhat easier, but forcing schools into the initial enrollment process raises serious issues.²⁹⁴ Do we really want schools to serve as DMVs for our children? Do we want to divert school time and resources away from the core goal of educating children and toward this mission? Do we want more school records or information about our kids being accessed or put online? What happens when those records are compromised? Finally, what sort of liability will be imposed on schools if that happens?

Parental permission-based systems have similar shortcomings as an initial enrollment process.²⁹⁵ If the parent-child relationship cannot be definitively established, fraud is possible. How do we guarantee that the parent or guardian is who they claim to be? How burdensome will site enrollment mandates be for both SNS operators as well as parents and guardians? Will the barriers to site enrollment force previously free SNS to begin charging fees? That could particularly disadvantage low-income families and youths.

4. The Identity/Data Transferability (“Subsequent Visit”) Problem

Even if we could solve the initial enrollment problem addressed above, age verification could also break down at the *subsequent visit* stage. This is true regardless of what initial enrollment process is used (e.g., national ID cards, school-based authentication, or parental permission-based systems).

²⁹⁴ See Adam Thierer, “Age Verification Debate Continues; Schools Now at Center of Discussion,” *Technology Liberation Front* blog, September 28, 2008, <http://techliberation.com/2008/09/25/age-verification-debate-continues-schools-now-at-center-of-discussion>

²⁹⁵ See Berin Szoka and Adam Thierer, “COPPA 2.0: The New Battle over Privacy, Age Verification & Online Safety,” The Progress & Freedom Foundation, *Progress on Point* No. 16.11, April 2009, (forthcoming)

Once minors are given credentials or digital tokens, how do we prevent them from sharing or selling their credentials? Similarly, how do we prevent older siblings from sharing their credentials with younger siblings? What would be the penalty for them doing so? Is there any way to prevent predators with children from using their own child's credentials to gain access to a SNS?

5. The Scale Problem

Age verification solutions are unlikely to work on "Internet scale." That is, the volume and breadth of Internet activity will significantly complicate age verification mandates. For example, can we expect *every* user or parent to go through the steps necessary to "verify" themselves or their kids for everything defined as having a SNS component? Can we expect every school, regardless of size or resources, to work within the chosen system and comply with its mandates? Importantly, this "scale problem" is significantly complicated by factors #6 and #7 below.

6. The Definitional Problem

How broadly will "social networking sites" be defined? Will chat rooms, hobbyist sites, instant messaging, video sharing sites, online marketplaces or online multiplayer gaming sites qualify as SNS? If so, how will they be policed and how burdensome will authentication mandates become for smaller sites? Will parents be willing to fill out potentially hundreds of forms (either online or off) and provide a host of additional facts about themselves or their children to all these sites? Again, what will such mandates mean for smaller websites?

7. The Offshore Problem

How would mandatory age verification work for a global, borderless platform like the Internet? Even if domestic social networking operators don't flee, many users *will* likely seek

out offshore sites to evade domestic regulations. Those offshore sites are often not as accountable to users or law enforcement as domestic sites, creating new risks for users. How could U.S. officials quarantine domestic SNS sites and users so that they cannot evade domestic age verification regulations?

8. The Resource Misallocation Problem

Lawmakers should realize that increased online regulation could divert resources from other problems or objectives. We do not live in a world of unlimited resources. Focusing on education and awareness-building efforts—especially K-12 online safety and media literacy education—is likely to provide much greater bang for the buck than mandatory age verification regulations.

9. The Speech Rights Problem

How do we balance the First Amendment-related values at stake here—for both adults and children? Are we treating minors as guilty until proven innocent by making it so difficult for them to communicate with each other in online communities? Minors do have *some* speech rights—although they are certainly not equivalent to those of adults. Regardless of the legal treatment of speech by minors, it just doesn't seem wise to stifle communication by minors in SNS environments, even when it is of an anonymous nature.

10. The Privacy Problem

It also seems unwise for lawmakers to require that even more personal information be put online—about kids, no less!—at a time when identity theft continues to be a major problem.²⁹⁶ Many parents today, like me, encourage their kids to put *zero* information about

²⁹⁶ The Identity Theft Resource Center, which has been tracking data security breaches for many years, recently reported that data breaches increased dramatically in 2008. According to its website, 656 data

themselves online because we believe that will keep them safer. AV mandates are at cross-purposes with that goal.

D. Summary of Potential Problems with Age Verification Mandates

In sum, the danger of mandatory age verification as a solution to online child safety concerns is that it will:

- result in unintended consequences or solutions that don't solve the problems they were intended to address; and,
- create a false sense of security that might encourage some youngsters (or adults) to let their guard down while online.

The Commission should heed the ISTTF's wise conclusion that "there is no one technological solution or specific combination of technological solutions to the problem of online safety for minors" and ISTTF's caution "against overreliance on technology in isolation or on a single technological approach."²⁹⁷ While the Task Force found that "technology can play a helpful role," it ultimately concluded that:

a combination of technologies, in concert with parental oversight, education, social services, law enforcement, and sound policies by social network sites and service providers may assist in addressing specific problems that minors face online. All stakeholders must continue to work in a cooperative and collaborative manner, sharing information and ideas to achieve the common goal of making the Internet as safe as possible for minors.²⁹⁸

breaches were reported by the end of 2008, reflecting an increase of 47% over the previous year's total of 446. "ITRC 2008 Breach List," December 31, 2008, www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml. Also see: "2006 Identity Theft Survey Report," Prepared for the Federal Trade Commission by Synovate, November 2007, www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

²⁹⁷ Final Report of the ISTTF at 6.

²⁹⁸ *Id.*

VI. THE IMPORTANCE OF HOUSEHOLD MEDIA RULES

It is important to realize that household-level rules and informal parental control methods often represent the most important steps that most parents can take in dealing with potentially objectionable content or teaching their children how to be sensible, savvy media consumers. Indeed, to the extent that many households never take advantage of the technical controls outlined above, it is likely because they rely instead on the informal household media rules.

A 2003 Kaiser Family Foundation survey found that “Almost all parents say they have some type of rules about their children’s use of media.”²⁹⁹ More recent Kaiser surveys have bolstered that finding. For example, a 2006 Kaiser survey of families with infants and preschoolers revealed that 85% of those parents who let their children watch TV at that age have rules about what their child can and cannot watch.³⁰⁰ Of those parents, 63% say they always enforce those rules. About the same percentage of parents said they had similar rules for video game and computer usage. Likewise, a June 2007 Kaiser poll revealed that:³⁰¹

- 65% of parents say they closely monitor their children’s media use;
- 73% of parents say they know a lot about what their kids are doing online;
- 87% of parents check their children’s instant messaging “buddy lists;”
- 82% of parents review their children’s social networking sites; and,
- 76% of parents look to see what websites their children have visited.

²⁹⁹ *Zero to Six: Electronic Media in the Lives of Infants, Toddlers and Preschoolers*, Kaiser Family Foundation, Fall 2003, p. 9, available at www.kff.org/entmedia/entmedia102803pkg.cfm

³⁰⁰ *The Media Family: Electronic Media in the Lives of Infants, Toddlers, Preschoolers and Their Parents*, Kaiser Family Foundation, May 2006, p. 20, www.kff.org/entmedia/7500.cfm

³⁰¹ Victoria Rideout, *Parents, Children & Media*, Kaiser Family Foundation Survey, June 2007, www.kff.org/entmedia/entmedia061907pkg.cfm

Similarly, a poll commissioned by Common Sense Media and Cable in the Classroom revealed that 85% of parents and legal guardians of children ages 6 to 18 who go online say they have talked to their child in the past year about how to be safe and smart online.³⁰²

Parents use a wide variety of household media consumption rules. Some can be quite formal in the sense that parents make clear rules and enforce them routinely in the home over an extended period of time. Other media consumption rules can be fairly informal, however, and are enforced on a more selective basis. Regardless, these household media consumption rules can be grouped into four general categories: (1) “where” rules; (2) “when and how much” rules; (3) “under what conditions” rules; and, (4) “what” rules.

A. “Where” Rules

One of the most important steps that parents can take to better control their children’s media usage is to establish firm rules regarding where their children can do so. “We don’t have to say no to having TVs, video games, or computers in our homes,” argues Dr. David Walsh, president and founder of the National Institute on Media and the Family, “but we should say no to where some of the screens go.”³⁰³

For example, parents can assign a specific television or computer for most media usage and then take steps to ensure that those devices have screening or filtering controls installed and programmed. Additionally, parents can require that their children consume media (TV, Internet, video games, *etc.*) in a specific room or area of the house where they can keep an eye or ear on what their kids are doing.

³⁰² “New Poll Finds That Parents Are Taking Proactive Steps to Keep Kids Safe and Smart on the Web,” Common Sense Media *Press Release*, September 25, 2007,

³⁰³ David Walsh, *No: Why Kids—of All Ages—Need to Hear It and Ways Parents Can Say It* (New York: Free Press, 2007), p. 269.

At a minimum, parents can start by at least getting televisions, computers, and game consoles out of kids' bedrooms so they can better monitor media usage by their children. According to a 2005 Kaiser survey, 68% of 8 to 18 year-olds have televisions in their bedrooms.³⁰⁴ Parents who let their kids lock themselves in their rooms with media devices have surrendered their first line of defense in protecting their children from potentially objectionable content.³⁰⁵ Luckily, the reverse appears to be true for computers. A 2006 Pew Internet & American Life Project survey of media usage by teenagers revealed that 74% of homes with teenagers have their computers in an "open family area."³⁰⁶ That result was consistent with Pew surveys taken in 2004 and 2000.

B. "When and How Much" Rules

Parents can also limit the overall number of hours that children can consume various types of media content, or when they can do so. (Several technological tools mentioned in Part III can help parents accomplish this.) For example, parents can impose restrictions on the times of the day that children can consume media with rules like, "No TV or video games after 8:00 PM," or, more stringently, "No TV or games on a school night." The 2007 Pew Internet & American Life Project survey mentioned above found that 58% of parents limit the amount of time their children can spend watching television; 59% limit how much time their kids can play

³⁰⁴ *Generation M: Media in the Lives of 8-18 Year-Olds*, Kaiser Family Foundation, March 2005, p. 10, www.kff.org/entmedia/entmedia030905pkg.cfm

³⁰⁵ "One of the most beneficial Nos is to keep TVs, video games, or computers out of kids' bedrooms. Sending your kid to her room isn't a punishment when she can catch up on her favorite shows or 'whatever else is on.' Once her door is closed, you don't know where your child goes on the Internet, what she is watching, or for how long. Keeping media out of the bedroom increases school performance and decreases the risk of obesity. Say yes to screens in a common space in the house. This may be a bit nosey, but it will help you keep track of your kids' screen time and virtual activities." Walsh, *op. cit.*, pp. 269-270.

³⁰⁶ Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew Internet & American Life Project, April 18, 2007, p. 8, www.pewinternet.org/PPF/r/211/report_display.asp

video games; and 69% limit how much time their children can spend online.³⁰⁷ A 2008 survey conducted by the Entertainment Software Association revealed an even greater degree of parental involvement, finding that 80% of parents have placed time limits on video game playing in their homes.³⁰⁸

C. “Under What Condition” Rules

“When and how much” rules represent a carrot-and-stick approach to media consumption / exposure. Parents can incentivize their children by requiring that other tasks or responsibilities be accomplished before media consumption is permitted. For example, many of us are familiar with this very common household media rule: “You have to finish your homework before you get to watch any TV.” Similar rules can be used for video games and other types of media.³⁰⁹

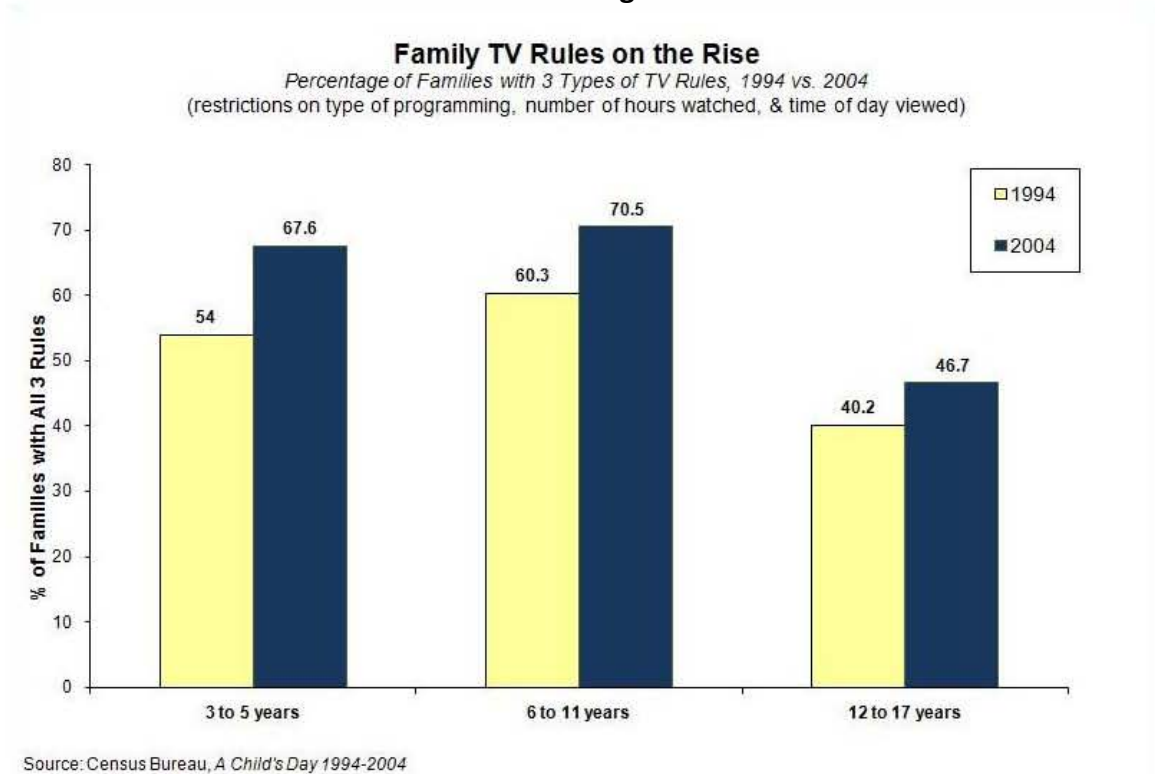
More creatively, parents can formulate a “media allowance” for their children (especially as they get older) to allow them to generally consume the media they want but only within certain boundaries. Again, incentives can be used with this approach. For example, better grades at school might be rewarded by adding one more hour of media time to their overall weekly media allowance.

³⁰⁷ *Id.*, p. 9.

³⁰⁸ *Essential Facts about the Computer and Video Game Industry: 2008 Sales, Demographics and Usage Data*, Entertainment Software Association, 2008, p. 8, www.theesa.com/facts/pdfs/ESA_EF_2008.pdf

³⁰⁹ My mother effectively used a conditional media rule with me as a child when she rewarded weekly achievement in school by letting me pick out a comic book at a local pharmacy. On the weeks that I didn’t do so well in school, I didn’t get my *Batman* or *Spiderman* fix!

Exhibit 43: More Families Using Household Media Rules



The U.S. Census Bureau recently released data on child-parent interaction that illustrates how the use of household media rules appears to be growing. The Census Bureau's data is part of a regular report entitled *A Child's Day*.³¹⁰ The last *Child's Day* report was conducted in 1994, and the most recent one in 2004, but the data for 2004 was just recently released. The latest results are very encouraging and reveal that, "Parents are taking a more active role in the lives of their children than they did 10 years ago," according to a Census Bureau press release.³¹¹ Parents are crafting more TV rules for their kids today than they were

³¹⁰ www.census.gov/population/www/socdemo/2004_detailedtables.html

³¹¹ "Parents More Active in Raising Their Children; More Children Get Television Restrictions," U.S. Census Bureau *Press Release*, October 31, 2007, www.census.gov/Press-Release/www/releases/archives/children/010850.html

in the past.³¹² The survey also found that parents were reading to their kids more and enrolling their children in more extracurricular activities and lessons.

D. “What” Rules

The efforts described above represent commonsense approaches parents can use to establish basic ground rules about how media are consumed in the home. But what about the substance of the media that are being consumed within these pre-established boundaries? This represents the fourth, and most important, category of household media rules: “what” rules.

Parents regularly enforce household rules about what their children can watch, listen to, play, or surf. For example, a poll conducted by the group TV Watch in June 2007 found that 73 percent of parents monitor what their children watch, including 87 percent of parents whose children are ages 0-10.³¹³ Similarly, according to the Pew Internet & American Life Project, 77 percent of parents already have rules for which TV shows their kids can watch, 67 percent have rules for the kinds of video games they can play, and 85 percent have rules about which Internet websites they can and cannot visit.³¹⁴ Another poll commissioned by Common Sense Media and Cable in the Classroom revealed that more than 93 percent of parents of children ages 6 to 18 who go online say they have taken action to make sure the Web sites their kid visits meets with their approval.³¹⁵

³¹² See Adam Thierer, “Latest Census Numbers on Kids, Parents & Media,” Progress & Freedom Foundation, *PFF Blog*, December 14, 2007, http://blog.pff.org/archives/2007/12/latest_census_n.html

³¹³ *TV Watch Survey of Parents*, Hart Research, June 2007, www.televisionwatch.org/junepollresults.pdf

³¹⁴ *Teens, Privacy, and Online Social Networks*, op. cit., p. 9.

³¹⁵ “New Poll Finds That Parents Are Taking Proactive Steps to Keep Kids Safe and Smart on the Web,” Common Sense Media Press Release, September 25, 2007, www.common sense media.org/news/press-releases.php?id=86

VII. THE ROLE OF THIRD-PARTY PRESSURE, RATINGS AND ADVICE

A. The Power of Public Pressure & Social Norms

Parents can, and do, work with others to influence media content before it comes into the home, or rely on other groups they trust to help them better understand what is in the media they are considering bringing into the home.³¹⁶ Parents can pressure media providers and programmers directly through public campaigns, or indirectly through advertisers.³¹⁷ As child development experts Jeanne Brooks-Gunn and Elisabeth Hirschhorn Donahue argue, “Because government will probably not intervene in the realm of media content, the most effective pressure on industry to produce positive media content will come from the court of public opinion made up of child advocates and, especially, families.”³¹⁸ In other words, the combination of social norms, press attention, public pressure, and even shame can act as a powerful influence on the composition of media content.

Consider the “watchdog” role played by groups like the Parents Television Council, Morality in Media, Common Sense Media, and the National Institute on Media and the Family. These groups can play a constructive role in influencing content decisions through the pressure they can collectively bring to bear on media providers in the marketplace. For example,

³¹⁶ As Competitive Enterprise Institute analysts Cord Blomquist and Eli Lehrer argue, “ratings systems will never substitute for other social institutions. Parents, houses of worship, schools, and communities need to take the lead in keeping obscene, dangerous, or offensive materials away from children. Ratings systems cannot be expected to do this. Properly constructed, they provide useful information to parents, nothing more and nothing less.” Cord Blomquist and Eli Lehrer, “Politically Determined Entertainment Ratings and How to Avoid Them,” Competitive Enterprise Institute *Issue Analysis* 2007 No. 12, December 2007, p. 25, <http://cei.org/pdf/6292.pdf>

³¹⁷ “There is every reason to believe that the marketplace, speaking through advertisers, critics, and self-selection by viewers, provides an adequate substitute for Commission involvement in protecting children and adults from television’s ‘captive’ quality.” Mark S. Fowler and Daniel L. Brenner, “A Marketplace Approach to Broadcast Regulation,” *Texas Law Review*, Vol. 60, No. 2, February 1982, p. 229.

³¹⁸ Jeanne Brooks-Gunn and Elisabeth Hirschhorn Donahue, “Introducing the Issue,” in *Children and Electronic Media, The Future of Children*, Vol. 18, No. 1, Spring 2008, p. 9.

Morality in Media's website outlines several strategies parents can use to influence advertisers, programming executives, and cable operators before resorting to calls for censorship. To allow parents to pressure advertisers, the group publishes a book listing the top 100 national advertisers, with addresses, phone and fax numbers, names of key executives, and their products, along with a products list cross-referenced to the manufacturer. The group produces a similar book that lists the names and addresses of the CEOs of the leading broadcast and cable companies in America so that viewers or listeners can complain directly to them.³¹⁹

Similarly, the Parents Television Council (PTC) awards its "seal of approval" to advertisers who only support programs that the PTC classifies as family-friendly.³²⁰ PTC also encourages parents to send letters and e-mails to advertisers who support programming they find objectionable and encourage those advertisers to end their support of those shows.

Such efforts have been effective at changing corporate behavior in other contexts. For example, in late 2006, after years of pressure from various health groups and average parents, 10 major food and beverage companies announced new, self-imposed restrictions on advertising to children. These 10 companies, which included McDonald's, Coca-Cola, Pepsi, Kraft Foods, and Hershey, account for more than two-thirds of all food and beverage advertising aimed at children.³²¹ Among their commitments, they agreed to not advertise products in schools; devote half their advertising to promoting healthier lifestyles and foods; limit the use of popular third-party characters (such as cartoon characters) in their ads; and

³¹⁹ Robert Peters, "The Importance of Making Complaints," Morality in Media website, available at www.moralityinmedia.org

³²⁰ www.parentstv.org/PTC/awards/main.asp

³²¹ Betsy McKay and Janet Adamy, "Food Companies Vow to Tighten Limits on Kids' Ads," *Wall Street Journal*, November 15, 2006, p. B3.

limit ads seen in interactive video games or promote healthy alternatives in those ads. The initiative will be monitored by the Council of Better Business Bureaus, which helped craft the agreement. The efforts appear to be making a difference.³²²

If public pressure can help change corporate attitudes and outputs when it comes to food and beverage advertising, there is every reason to believe that it can also change other types of media behavior. Consider some examples of how it already has made a difference:

- In late 2006, intense public pressure forced News Corp. to abandon the publication of a controversial book by O.J. Simpson in which he described how he might have killed his ex-wife and her friend.³²³ *Washington Post* columnist Shankar Vedantam argued that this episode “showed that shame remains a powerful tool in America.”³²⁴
- In April 2007, radio talk show host Don Imus had his CBS Radio show and MSNBC television program canceled after making offensive remarks about the Rutgers University women’s basketball team.³²⁵ Public outcry was so intense that almost all his largest advertisers pulled their support for his show less than a week after the incident occurred.³²⁶ (Of course, Imus did end up back on the air before the end of the year!)
- In 2008, MTV began casting a new reality show called *Model Maker*, which sought woman ages 17 to 24 who would compete by engaging in extreme weight loss and body makeovers. An intense backlash ensued, led by the public health community. As *USA Today* reported, “Thankfully, MTV is nixing the show after complaints from, among others, the National Association of Anorexia Nervosa and Association of Eating Disorders and a British parliamentary group. The outcry is the latest hopeful marker that society’s attitudes to unnatural thinness are slowly changing, much as smoking has become socially dubious.”³²⁷

³²² See Susan Levine and Lori Aratani, “Sweet Surrender,” *Washington Post*, May 22, 2008, p. D1, www.washingtonpost.com/wp-dyn/content/article/2008/05/21/AR2008052102827.html

³²³ Tim Harper, “O.J. Book, Fox Show Cancelled,” *Toronto Star*, November 21, 2006.

³²⁴ Shankar Vedantam, “Abandoned O.J. Project Shows Shame Still Packs a Punishing Punch,” *Washington Post*, November 27, 2006, p. A2.

³²⁵ Bill Carter and Jacques Steinberg, “CBS Drops Imus Radio Show over Racial Remark,” *New York Times*, April 12, 2007, www.nytimes.com/2007/04/12/business/media/12cnd-imus.html?ex=1180756800&en=15850df43f6b8c51&ei=5070; Matthew Robinson, “U.S. Radio Host Imus Hints Career May Be Ending,” *The Guardian*, April 12, 2007, <http://sport.guardian.co.uk/breakingnews/feedstory/0,-6552506,00.html>

³²⁶ Kenneth Li, “Here’s Why MSNBC Dropped Imus,” *Reuters*, April 11, 2007, <http://blogs.reuters.com/2007/04/11/heres-why-msnbc-dropped-imus>

³²⁷ “Dangerous ‘Model’,” *USA Today*, October 24, 2008, P, 10A.

Parents and other organizations might also be able to work together to pressure content providers or distributors to self-regulate materials that cannot be blocked with parental control technologies. For example, some parents feel in-flight movies shown on drop-down screens in airplanes contain sexual or violent themes unfit for some younger viewers; unfortunately, there is no way for them to block the screen or turn off those videos. KidSafeFilms.org is a new group that pressures airline operators to take steps to further restrict or edit what is shown in the open cabin space since parents have no control over it.³²⁸ Of course, eventually most airlines will have individual screens for each seat and parents will be able to control what is being viewed by their children. But the efforts of KidsSafeFilms.org might help speed up those efforts and get airlines to be more selective about the content they show on drop-down screens in the meantime.³²⁹ A similar effort might be useful in terms of discouraging advertising for potentially offensive content on television, or at least encouraging programmers to air such ads during later hours of the day.

B. Independent Media Rating Efforts

Most parents, however, will not likely feel the need to pressure media producers directly but instead simply want better information about the media they bring into the home. Or they might feel comfortable getting independent advice or third-party ratings about various types of media content. Several “independent” rating groups exist that fill this need:

- Common Sense Media’s comprehensive website³³⁰ allows both parents and children to rate a diverse assortment of media content and then sort it all by age group to find what

³²⁸ www.kidsafefilms.org

³²⁹ Adam Thierer, “Long-Range Censors,” *City Journal*, October 3, 2007, www.city-journal.org/html/eon2007-10-03at.html

³³⁰ www.common sense media.org

is appropriate for their families.³³¹ The site also offers parental tips such as its “Managing Media: Downloads, Internet TV, and More” checklist, which helps parents manage their children’s media consumption.³³² Importantly, Common Sense Media also partners with retail stores, online providers, and technology vendors to better inform parents about what to expect in the media their kids consume. For example, Common Sense Media has a partnership with Best Buy to feature the organization’s video game and DVD reviews, content descriptions and user comments in the relevant sections of BestBuy.com website.

- The National Institute on Media and the Family’s MediaWise website offers occasional columns and newsletters for parents that include information they can use to make more informed judgments about the content their children consume.³³³ In particular, the institute’s website offers a free “KidsScore” system³³⁴ that rates thousands of movies, TV shows, video games. All content is alphabetized and easy to search.
- Focus on the Family’s *Plugged In* magazine and Plugged In Online website³³⁵ are independent rating resources “designed to help equip parents, youth leaders, ministers, and teens with the essential tools that will enable them to understand, navigate, and impact the culture in which they live.”³³⁶ Because of the group’s religious focus, its movie, television, and music reviews also probe the spiritual content found in some media titles. The Parent Previews website³³⁷ reviews new movies, DVDs and video games on an easy-to-understand A-F grading system. Four primary categories are graded (violence, sexual content, language and drug or alcohol use) to determine the title’s overall grade.

³³¹ Joe Garofoli, “Media Guide Offers Reviews for Parents—But No Soapbox,” *San Francisco Chronicle*, December 8, 2006, <http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/12/08/MNG75MS23C1.DTL>

³³² www.commonsensemedia.org/parent_tips/commonsense_view/index.php?id=232

³³³ www.mediafamily.org

³³⁴ www.mediafamily.org/kidscore

³³⁵ www.pluggedinonline.com

³³⁶ www.pluggedinonline.com/aboutUs/index.cfm

³³⁷ www.parentpreviews.com

Exhibit 44: Independent Media Reviews and Rating Systems

Common Sense Media



Media Wise "KidScore"



Plugged In Online



Parents Preview



Other creative, independent rating systems are on the market or being developed. For example, in March 2006, TiVo announced a partnership with the Parents Television Council, the Parents Choice Foundation and Common Sense Media to jointly develop TiVo KidZone.³³⁸ Using ratings and information created by those groups, KidZone will allow parents to filter and record

338 www.tivo.com/whatistivo/tivois/tv/index.html#kid_zone

only *the content* that those groups deem appropriate.³³⁹ All these private, voluntary education and rating methods are preferable to the type of pressure that some groups bring to bear in the *political* marketplace when they encourage policymakers to regulate media content.³⁴⁰

Exhibit 45: Industry-Supported Efforts that Highlight Parental Controls

The TV Boss



Pause Parent Play



Control Your TV.org



Take Parental Control



³³⁹ Saul Hansell, "TiVo to Offer Tighter Rein on Children's Viewing," *New York Times*, March 2, 2006, www.nytimes.com/2006/03/02/technology/02tivo.html?_r=1&oref=slogin

³⁴⁰ See Adam Thierer, "Examining the FCC's Complaint-Driven Broadcast Indecency Enforcement Process," Progress & Freedom Foundation *Progress on Point* 12.22, November 2005, www.pff.org/issues-pubs/pops/pop12.22indecencyenforcement.pdf

Finally, there are several other excellent websites supported by media enterprises that offer parents excellent advice on media ratings and parental controls, such as: TV Watch,³⁴¹ The TV Boss.org,³⁴² Pause-Parent-Play,³⁴³ Control Your TV.org,³⁴⁴ and Take Parental Control.org.³⁴⁵

VIII. THE POWER OF THE PURSE AND MEDIA ALLOWANCES

It is important that the Commission not forget what, at times, constitutes the ultimate parental control tool: the “power of the purse.” In most cases, when kids want to consume a certain type of media—or even consume something they see advertised in the media—they need money to do so. Televisions, movies, video games, cell phones, computers, portable music players, Internet connections, and so on, do not just drop from high-tech heaven into our kids’ laps!³⁴⁶ When kids want those things—or want things that are advertised on those media platforms—they must go to their parents and ask them for money. And, although at times it may be difficult, all parents have the power to say “No.”³⁴⁷

Parents can, and do, establish media budgets to better control what their kids see, hear, or play.³⁴⁸ Many of the technologies discussed in Section III can facilitate the creation and

³⁴¹ www.televisionwatch.org

³⁴² www.thetvboss.org

³⁴³ www.pauseparentplay.org

³⁴⁴ www.controlyourtv.org

³⁴⁵ <http://takeparentalcontrol.org>

³⁴⁶ Indeed, many of these technologies and types of media are out of the financial reach of most kids. Most new video games cost \$40-\$60 per title. DVDs are \$10-\$25. Cable subscriptions run at least \$50 per month. While most websites are free, the computers and Internet connections needed to access them are not. Finally, most kids can’t afford cell phones and monthly subscriptions, and they are not old enough to sign up for service anyway. So parents must be involved in all these media decisions.

³⁴⁷ See David Walsh, PhD, *No: Why Kids—of All Ages—Need to Hear It and Ways Parents Can Say It* (New York: Free Press, 2007).

³⁴⁸ See Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), pp. 8-9.

enforcement of such household media budgets or allowances. Many new parental control tools incorporate sophisticated bill monitoring and spending control tools. For example, most TV set-top boxes, video game consoles, and cell phones have tools that can limit media spending or at least give parents a clear report on how much money has been spent. These tools can help parents enforce whatever media budget they establish for their children.

IX. JURISDICTIONAL AND FIRST AMENDMENT CONSIDERATIONS

A. Jurisdictional Considerations

While the Commission is merely carrying out the study required by a congressionally enacted statute, there are unanswered questions about the delegation of such authority when the subject matter in question is well outside the agency's traditional jurisdiction. For example, the Commission's *Notice* mentions video games or virtual worlds, online video distribution networks or video hosting sites, mobile web content, MP3 players or iPods, P2P networks, VCRs or DVD players, PVRs or TiVo, Internet filters, safe search tools, laptops, and so on. From a jurisdictional perspective, it is unclear how much authority the Commission has to study—let alone exercise oversight authority over—those industries and technologies.

This much *is* clear, however: The Commission certainly has no authority under the Communications Act or any other statute to directly *regulate* those media technologies or platforms. To the agency's credit, however, no suggestion has been made in the *Notice* that regulation is being considered.

B. First Amendment Constraints

One might argue that merely *studying* the marketplace for “advance blocking controls” raises no serious First Amendment concerns. The Commission's regulatory powers, however,

often do come into conflict with the First Amendment’s general prohibition against meddling—even indirectly—with free speech and artistic expression.

In considering the effectiveness of various blocking controls or parental control tools, the Commission should consider the extent to which mandated regulatory alternatives might raise serious First Amendment objections and, consequently, be the subject of court challenges. That’s especially the case in light of recent First Amendment case law emanating from the Internet and video game sectors.

1. Modern First Amendment Jurisprudence Has Acknowledged New Technological Capabilities for Individual / Household Empowerment

Until very recently it has been difficult for individual households to tailor media content to their specific needs or values. In essence, the off button on TVs and radios was the only technical control at a parent’s disposal in the analog era. In that environment, many believed that government needed to act as a surrogate for parents because of the lack of control families had over their media decisions and encounters. In other words, because it was difficult for families to enforce their own “household standards,” the government would step in and create a baseline—quite amorphous and sometimes completely arbitrary—“community standard” for the entire nation. That community standard would be enforced by law and treat all households as if they had the same tastes or values.

For example, in the context of broadcast television and radio programming, the Supreme Court famously held in *FCC v. Pacifica* (1978) that FCC oversight and regulatory penalties (*e.g.*, fines or license revocation) would help prevent “uninvited” programming from

acting as an “intruder” into the home.³⁴⁹ By a slim 5-4 margin, that logic became the law of the land for broadcasting and remains so today. The Commission’s regulatory powers in this field are still driven by that logic³⁵⁰ even though it is being hotly contested in the courts currently.³⁵¹

Similar arguments would be put forward by policymakers in the mid-1990s when they sought to impose restrictions on Internet and video game content. Courts have rejected these efforts, however. In striking down the Communications Decency Act’s effort to regulate underage access to adult-oriented websites, the Supreme Court declared in *Reno v. ACLU* (1997) that a law that places a “burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving” the same goal.³⁵² And several lower courts have rejected regulation of video game content on similar grounds.³⁵³

What is most interesting about these recent Internet and video game decisions is that the same logic could be applied to many other types of media outlets and content—including broadcasting. Indeed, as was revealed in Section III, many “less restrictive alternatives” are available to parents today to help them shield their children’s eyes and ears from content they might find objectionable, regardless of what that content might be.

If it is the case that families now have the ability to effectively tailor media consumption to their own preferences—that is, to craft their own “household standards”—the regulatory

³⁴⁹ *FCC v. Pacifica Foundation*, 438 U.S. 726, 727-8 (1978).

³⁵⁰ See Adam Thierer, “Why Regulate Broadcasting: Toward a Consistent First Amendment Standard for the Information Age,” Catholic University Law School *CommLaw Spectus*, vol. 15, pp. 431-482, Summer 2007; http://commlaw.cua.edu/articles/v15/15_2/Thierer.pdf

³⁵¹ See Adam Thierer, “FCC v. Fox and the Future of the First Amendment in the Information Age,” *Engage*, February 2009, www.fed-soc.org/doclib/20090216_ThiererEngage101.pdf

³⁵² *Reno v. ACLU*, 521 U.S. 844 (1997).

³⁵³ See Adam Thierer, “Fact and Fiction in the Debate over Video Game Regulation,” Progress & Freedom Foundation *Progress Snapshot* 13.7, March 2006, www.pff.org/issues-pubs/pops/pop13.7videogames.pdf

equation should also change: Regulation can no longer be premised on the supposed helplessness of households to deal with content flows if families have been empowered and educated to make content determinations for themselves.

In fact, in another recent decision, the Supreme Court confirmed that this would be the new standard to which future government regulations of media content would be held. In *United States v. Playboy Entertainment Group* (2000),³⁵⁴ the Court struck down a law that required cable companies to “fully scramble” video signals transmitted over their networks if those signals included any sexually explicit content. Echoing its earlier holding in *Reno v. ACLU*, the Court found that “less restrictive” means were available to parents looking to block those signals in the home. Specifically, in *Playboy* case, the Court argued that:

[T]argeted blocking [by parents] enables the government to support parental authority without affecting the First Amendment interests of speakers and willing listeners—listeners for whom, if the speech is unpopular or indecent, the privacy of their own homes may be the optimal place of receipt. Simply put, targeted blocking is less restrictive than banning, and the Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests.³⁵⁵

More importantly, the Court held that:

It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time. A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act.³⁵⁶

Thus, the Supreme Court has set an extraordinarily high bar for policymakers seeking to regulate modern media content. Not only is it clear that the Court is increasingly unlikely to allow the extension of broadcast-era content regulations to new media outlets and

³⁵⁴ *United States v. Playboy Entertainment Group*, 529 U.S. 803 (2000).

³⁵⁵ *Id.* at 815.

³⁵⁶ *Id.* at 824.

technologies, but it appears certain that judges will apply much stricter constitutional scrutiny to *all* efforts to regulate speech and media providers in the future, including broadcasting. As constitutional law scholar Geoffrey R. Stone of the University of Chicago School of Law has noted:

The bottom line, then, is that even in dealing with material that is “obscene for minors,” the government cannot *directly* regulate such material... Rather, it must focus on empowering parents and other adults to block out such material at their own discretion, by ensuring that content-neutral means exist that enable individuals to exclude constitutionally protected material they *themselves* want to exclude. Any more direct regulation of such material would unnecessarily impair the First Amendment rights of adults.³⁵⁷

2. The Commission’s Authority to Regulate Content is Limited to Over-the-Air Broadcasting

Regardless of how pending court controversies come out, what remains beyond dispute is that the Commission’s ability to regulate media content is already tightly limited by its authority under the *Pacifica* regime. Consequently, while the Commission has the leeway to *study* advanced blocking technologies and methods for various media platforms, its content regulatory authority is limited to just one media delivery platform: over-the-air broadcasting.

Finally, because the vast majority of content for which blocking technologies are being considered here would be non-obscene in character, the constitutional bar would be even higher.

X. CONCLUSION

The Commission has an opportunity in this proceeding to conduct a great public service by:

³⁵⁷ Geoffrey R. Stone, “The First Amendment Implications of Government Regulation of ‘Violent’ Programming on Cable Television,” National Cable and Telecommunications Association, October 15, 2004, p. 10, www.ncta.com/ContentView.aspx?hidenavlink=true&type=lpubtp5&contentid=2881

- Expanding information and education about existing tools and rating systems;
- Examining new or independent tools and ratings systems parents might find useful (but *not* mandating them or tipping the balance against existing tools or rating systems); and
- Encouraging parents to use these tools and methods and to talk to their children about appropriate media use.

The jurisdictional and First Amendment limitations the Commission faces would limit its ability to impose regulations mandating advanced blocking technologies, universal ratings, or even restrictive parental control defaults. The Commission would be entirely safe, however, in recommending—or even immediately undertaking itself—a significant public education campaign.³⁵⁸ For example, there is no reason the agency could not create a compendium of the existing tools and rating systems and place that information on its website. The Commission could also create or sponsor public service announcements (PSAs) and tutorials that would run on major media outlets. Education is the low-cost, constitutionally “less restrictive,” and most long-lasting solution to the concerns the Commission is addressing in this matter.

Respectfully submitted,

/s/ Adam D. Thierer
The Progress & Freedom Foundation
1444 Eye St., NW Suite 500
Washington, DC 20005
202-289-8928
athierer@pff.org

April 16, 2009

³⁵⁸ In 1996, the Supreme Court struck down a Rhode Island ban on the advertising of alcohol prices because less restrictive alternatives were available to the state, such as an educational campaign or counter-advertising. *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 507-08 (1996).